



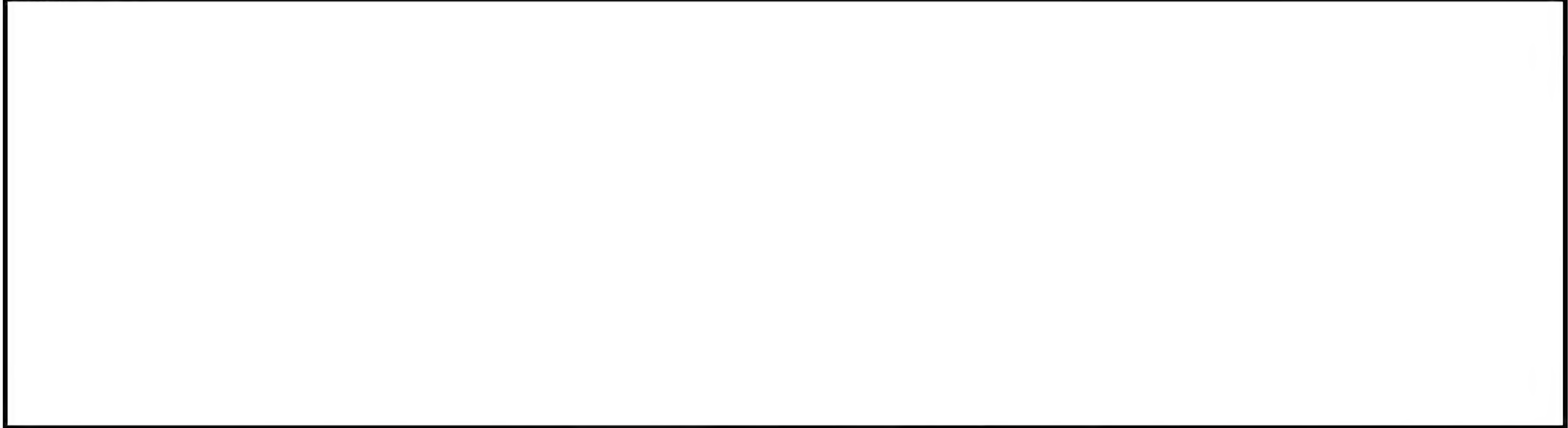
U.S. Department of Justice
Federal Bureau of Investigation

July, 2016
Washington, D.C.

CLINTON E-MAIL INVESTIGATION

MISHANDLING OF CLASSIFIED – UNKNOWN SUBJECT OR COUNTRY (SIM)

(S//NF)



b1
b3

This report recounts the information collected in this investigation. It is not intended to address potential inconsistencies in, or the validity of, the information related herein.



b3
b7E

(U//~~FOUO~~) On July 10, 2015, the Federal Bureau of Investigation (FBI) initiated a full investigation based upon a referral received from the US Intelligence Community Inspector General (ICIG), submitted in accordance with Section 811(c) of the Intelligence Authorization Act of 1995 and dated July 6, 2015, regarding the potential unauthorized transmission and storage of classified information on the personal e-mail server of former Secretary of State Hillary Clinton (Clinton).^a The FBI's investigation focused on determining whether classified information was transmitted or stored on unclassified systems in violation of federal criminal

^a (U//~~FOUO~~) For a complete listing of the interviews conducted, electronic media collected, legal process issued, and classified e-mails identified during this investigation, please refer to Appendices A-D. As background, Clinton was Secretary of State from January 21, 2009 through February 1, 2013.

statutes and whether classified information was compromised by unauthorized individuals, to include foreign governments or intelligence services, via cyber intrusion or other means. (U//~~FOUO~~) In furtherance of its investigation, the FBI acquired computer equipment and mobile devices, to include equipment associated with two separate e-mail server systems used by Clinton, and forensically reviewed the items to recover relevant evidence. In response to FBI requests for classification determinations in support of this investigation, US Intelligence Community (USIC) agencies determined that 81 e-mail chains,^{b,c} which FBI investigation determined were transmitted and stored on Clinton's UNCLASSIFIED personal server systems, contained classified information ranging from the CONFIDENTIAL to TOP SECRET/SPECIAL ACCESS PROGRAM levels at the time they were sent between 2009-2013. USIC agencies determined that 68 of these e-mail chains remain classified. In addition, the classification determination process administered by the US Department of State (State) in connection with Freedom of Information Act (FOIA) litigation identified approximately 2,000 additional e-mails currently classified CONFIDENTIAL and 1 e-mail currently classified SECRET, which FBI investigation determined were transmitted and stored on at least two of Clinton's personal server systems.^d

(U//~~FOUO~~) The FBI's investigation and forensic analysis did not find evidence confirming that Clinton's e-mail accounts or mobile devices were compromised by cyber means. However, investigative limitations, including the FBI's inability to obtain all mobile devices and various computer components associated with Clinton's personal e-mail systems, prevented the FBI from conclusively determining whether the classified information transmitted and stored on Clinton's personal server systems was compromised via cyber intrusion or other means. The FBI did find that hostile foreign actors successfully gained access to the personal e-mail accounts of individuals with whom Clinton was in regular contact and, in doing so, obtained e-mails sent to or received by Clinton on her personal account.

1. (U//~~FOUO~~) Clinton's Personal E-Mail Server Systems

A. (U//~~FOUO~~) Initial E-mail Server: June 2008 – March 2009

(U//~~FOUO~~) In or around 2007, Justin Cooper, at the time an aide to former President William Jefferson Clinton (President Clinton), purchased an Apple OS X server (Apple Server) for the sole purpose of hosting e-mail services for President Clinton's staff.^{1,2} Due to concern over ensuring e-mail reliability and a desire to segregate e-mail for President Clinton's various post-presidency endeavors, President Clinton's aides decided to maintain physical control of the Apple Server in the Clinton residence in Chappaqua, New York (Chappaqua residence).^{3,4,5} According to Cooper, in or around June 2008, a representative from Apple installed the Apple

^b (U//~~FOUO~~) The number of classified e-mail chains identified may change as classification determination responses continue to be returned to the FBI.

^c (U//~~FOUO~~) For the purposes of the FBI's investigation, an "e-mail chain" is defined as a set of e-mail responses having the same initial e-mail. The subject line may be edited in these chains to reflect the purpose of the forward or reply.

^d (U//~~FOUO~~) State did not provide a determination with respect to the classification of these e-mails at the time they were sent. According to State Under Secretary of Management, Patrick Kennedy, unclassified information provided to State in confidence can later be considered classified when it is "further assessed the disclosure of such information might damage national security or diplomatic relationships." Such information is referred to as "up-class" or "up-classified."

Server^e in the basement of the Chappaqua residence.^{6,7} The FBI was unable to obtain records from Cooper or Apple to verify the installation. At the time, Cooper was the only individual with administrative access to the Apple Server; however, the Clinton family and their Chappaqua residence staff had physical access to the Apple Server.^{8,9} The Apple Server initially hosted the domains presidentclinton.com and wjcoffice.com, which were used by President Clinton's staff.^{f,10,11}

(U//~~FOUO~~) Prior to January 21, 2009, when she was sworn in as the US Secretary of State, Clinton used a personally-acquired BlackBerry device with service initially from Cingular Wireless and later AT&T Wireless, to access her e-mail accounts.^{12,13} Clinton initially used the e-mail addresses hr15@mycingular.blackberry.net and then changed to hr15@att.blackberry.net.^{14,15} According to Cooper, in January 2009, Clinton decided to stop using her hr15@att.blackberry.net e-mail address and instead began using a new private domain, clintonemail.com, to host e-mail service on the Apple Server.¹⁶ Clinton stated to the FBI that she directed aides, in or around January 2009, to create the clintonemail.com account, and as a matter of convenience her clintonemail.com account was moved to an e-mail system maintained by President Clinton's aides.¹⁷ While Cooper could not specifically recall registering the domain, Cooper was listed as the point of contact for clintonemail.com when the domain was registered with a domain registration services company, Network Solutions, on January 13, 2009.^{18,19} Clinton used her att.blackberry.net e-mail account as her primary e-mail address until approximately mid-to-late January 2009 when she transitioned to her newly created hdr22@clintonemail.com account.^{20,21} The FBI did not recover any information indicating that Clinton sent an e-mail from her hr15@att.blackberry.net e-mail after March 18, 2009.

(U//~~FOUO~~) According to Cooper, in or around January 2009 the decision was made to move to another server because the Apple Server was antiquated and users were experiencing problems with e-mail delivery on their BlackBerry devices.^{22,23} At the recommendation of Huma Abedin, Clinton's long-time aide and later Deputy Chief of Staff at State, in or around fall 2008, Cooper contacted Bryan Pagliano, who worked on Clinton's 2008 presidential campaign as an information technology specialist, to build the new server system and to assist Cooper with the administration of the new server system.^{24,25,26,27} Pagliano was in the process of liquidating the computer equipment from Clinton's presidential campaign when Cooper contacted Pagliano about using some of the campaign's computer equipment to replace the existing Apple Server at Clinton's Chappaqua residence.^{28,29} Pagliano was unaware the server would be used by Clinton at the time he was building the server system; rather, he believed the server would be used by President Clinton's staff.³⁰ Clinton told the FBI that at some point she became aware there was a server in the basement of her Chappaqua residence.³¹ However, she was unaware of the transition from the Apple Server managed by Cooper to another server built by Pagliano and therefore, was not involved in the transition decision.³²

B. (U//~~FOUO~~) *Second E-mail Server: March 2009 – June 2013*

^e (U//~~FOUO~~) The Apple Server consisted of an Apple Power Macintosh G4 or G5 tower and an HP printer.

^f (U//~~FOUO~~) Investigation determined various employees of President Clinton maintained e-mail accounts using the presidentclinton.com domain to include

President Clinton did not maintain an e-mail account on the Apple Server. The e-mail domain wjcoffice.com was primarily a legacy domain that contained mostly forwarded e-mail.

(U//~~FOUO~~) Between the fall of 2008 and January 2009, Pagliano requisitioned the original hardware for the second e-mail server from Clinton's presidential campaign headquarters in Arlington, VA.³³ In addition to hardware acquired from Clinton's presidential campaign, Pagliano and Cooper^g purchased additional necessary equipment through commercial vendors.^{34,35,36,37} In March 2009, after Pagliano had acquired all of the server equipment and installed the necessary software, he and Cooper met at Clinton's Chappaqua residence to physically install the server and related equipment in a server rack in the Clintons' basement.^{h,38,39}

(U//~~FOUO~~) Once the new server systemⁱ was physically installed and powered on, Pagliano began migrating the e-mail data from the Apple Server to the Pagliano-administered server system (Pagliano Server).⁴⁰ Pagliano believed he "popped out" all of the e-mail from the Apple Server and that no e-mail content should have remained on the Apple Server once the migration took place.⁴¹ Pagliano stated to the FBI that he only transferred clintonemail.com e-mail accounts for Abedin and [redacted] from the Apple Server and said he was unaware of and did not transfer an e-mail account for Clinton.^{j,42} However, Cooper stated to the FBI that he believed Clinton had a clintonemail.com e-mail account on the Apple Server, and that Abedin did not have a clintonemail.com account on the Apple Server.⁴³ As the FBI was unable to obtain the original Apple Server for a forensic review for reasons explained below, the FBI cannot determine which clintonemail.com e-mail accounts were hosted on, and transferred from, the Apple Server to the Pagliano Server.

b6
b7C

(U//~~FOUO~~) After the e-mail account migration was completed, Cooper changed the Mail Exchange (MX) records^k to ensure that delivery of all subsequent e-mail to or from e-mail addresses on the presidentclinton.com and clintonemail.com domains would be directed toward the new Pagliano Server instead of the Apple Server.⁴⁴ The Pagliano Server was only used for e-mail management, and the FBI's review of the oldest available backup image of this server, dated June 24, 2013, did not indicate that any e-mail users' files were stored on the Pagliano Server.⁴⁵

(U//~~FOUO~~) In March 2009, following the e-mail migration from the Apple Server to the Pagliano Server, the Apple Server was repurposed to serve as a personal computer for household staff.⁴⁶ [redacted] at Clinton's Chappaqua residence, subsequently used the Apple Server equipment as a workstation.⁴⁷ In 2014, the data on the Apple computer was transferred to an Apple iMac computer, and the hard drive of the old Apple computer, which

b6
b7C

^g (U//~~FOUO~~) Cooper had [redacted] and was often responsible for reimbursing staff for purchases/expenses.

b6
b7C

^h (U//~~FOUO~~) Pagliano visited Clinton's Chappaqua residence on at least three occasions to work on the server: in March 2009, to install the server; in June 2011, to upgrade the equipment; and in January 2012, to fix a hardware issue.

ⁱ (U//~~FOUO~~) The Pagliano Server initially consisted of the following equipment: a Dell PowerEdge 2900 server running Microsoft Exchange for e-mail hosting and management, a Dell PowerEdge 1950 server running BlackBerry Enterprise Server (BES) for the management of BlackBerry devices, a Seagate external hard drive to store backups of the Dell PowerEdge 2900 server, a Dell switch, a Cisco firewall, and a power supply.

^j (U//~~FOUO~~) An e-mail obtained during the FBI investigation from Cooper to Clinton, indicated that in April 2009, Cooper was preparing to update Clinton's BlackBerry to "put it on our new system."

^k (U) An MX record determines which server will handle e-mail delivery for a domain and is necessary for routing e-mail to its proper destination.

previously served as the Apple Server was discarded.⁴⁸ On October 14, 2015, Williams & Connolly LLP (Williams & Connolly), counsel for Clinton, confirmed to the Department of Justice (DOJ) that a review of the iMac was conducted, pursuant to a request by DOJ, and no e-mails were found belonging to Clinton from the period of her tenure as Secretary of State.⁴⁹

(U//~~FOUO~~) Pagliano and Cooper both had administrative accounts on the Pagliano Server.⁵⁰ At Cooper's direction, Pagliano handled all software upgrades and general maintenance.⁵¹ Cooper described his role as "the customer service face," and he could add users or reset passwords on the e-mail server.⁵² Cooper and Pagliano both handled the acquisition and purchase of server-related items.⁵³ For example, in March 2009, Cooper registered a Secure Sockets Layer (SSL)¹ encryption certificate at Pagliano's direction for added security when users accessed their e-mail from various computers and devices.^{54,55} Clinton stated she had no knowledge of the hardware, software, or security protocols used to construct and operate the servers.⁵⁶ When she experienced technical issues with her e-mail account she contacted Cooper for assistance in resolving those issues.⁵⁷

(U//~~FOUO~~) Pagliano stated that a complete backup of the Pagliano Server was made on a Seagate external hard drive once a week and a differential backup^m was completed every day, and this continued from the initial Pagliano Server installation in March 2009 until June 2011 when the external hard drive was replaced.⁵⁸ As space on the hard drive ran out, backups were deleted on a "first in, first out" basis.⁵⁹ In June 2011, Pagliano replaced the Seagate external hard drive with a Cisco Network Attached Storage (NAS) device, to store backups of the server.⁶⁰ The FBI was unable to forensically determine how frequently the NAS captured backups of the Pagliano Server.

(U//~~FOUO~~) According to Pagliano, in early 2013, due to user limitations and reliability concerns regarding the Pagliano Server, staff for Clinton and President Clinton discussed future e-mail server options, and a search was initiated to find a vendor to manage a Clinton e-mail server.^{n, 61} Additionally, Pagliano's expressed desire to seek new employment contributed to the decision to move to a new server.⁶² A search for the new vendor was facilitated with the assistance of [REDACTED] Infograte, an information technology consulting company.^{63,64,65} [REDACTED] was introduced to Clinton's Chief of Staff, Cheryl Mills, on or about January 2, 2013 through a mutual business associate.⁶⁶ [REDACTED] stated she worked with Mills and Pagliano to produce a request for proposal which was used to solicit responses from multiple firms, including Denver-based information technology firm Platte River Networks (PRN).⁶⁷ Clinton recalled that the transition to the PRN Server was initiated by President Clinton's aides seeking a higher level of service than could be provided by the Pagliano Server.⁶⁸ Pagliano identified President Clinton's [REDACTED] as making the final decision to select PRN.⁶⁹ In the spring of 2013, PRN negotiated the terms of the contract to host e-mail services and eventually signed a Service Level Agreement on July 18, 2013.^{70,71}

b6
b7Cb6
b7C

¹ (U) SSL is a security protocol used to establish an encrypted connection between a server and another machine, allowing sensitive information such as login credentials or credit card information to be transmitted in an encrypted format instead of in plain text. SSL certificates, issued by a third-party Certificate Authority, are small files that must be installed on servers to establish secure sessions with web browsers.

^m (U) A differential backup is a cumulative backup of all changes that have occurred since the last full backup.

ⁿ (U//~~FOUO~~) The new Clinton e-mail server hosted e-mail for Clinton, President Clinton, [REDACTED] and their respective staffs.

b6
b7C

C. (U//~~FOUO~~) *Third E-mail Server: June 2013 – October 2015*

(U//~~FOUO~~) Following the selection of PRN to manage the Clintons' personal e-mail server and accounts, PRN's management assigned two PRN employees to handle the primary installation and administration of the third server system (PRN Server).⁷⁴ [REDACTED] who worked remotely from his home in [REDACTED] handled day-to-day administration for the PRN Server, and [REDACTED] who worked at PRN's headquarters in Colorado, handled all hardware installation and any required physical (i.e. "hands-on") maintenance for the PRN Server.^{75,76,77,78} During the transition to the PRN Server, [REDACTED] advised he worked with Pagliano to understand the existing architecture of the Pagliano Server.⁷⁴ As part of this transition process, on or around June 4, 2013, [REDACTED] was granted administrator access to the Pagliano Server, as well as any accompanying services, such as the domain registration services through Network Solutions.^{75,76,77,78}

b6
b7C

(U//~~FOUO~~) On June 23, 2013, [REDACTED] traveled to Clinton's Chappaqua residence, where he powered down the Pagliano Server and transported it to a datacenter in Secaucus, New Jersey, run by Equinix, Inc. (Equinix).^{79,80,81} The PRN Server remained at the Equinix facility until it was voluntarily produced to the FBI on October 3, 2015.^{82,83} The only equipment [REDACTED] left at the Chappaqua residence was the existing firewall and switch, since PRN intended to purchase its own firewalls and switches.⁸⁴ [REDACTED] reconnected and powered on the equipment for the Pagliano Server at the datacenter, so users could connect to their e-mail accounts,⁸⁵ and he continued to work at the datacenter for a few days setting up the remaining equipment^p for the PRN Server.⁸⁶ [REDACTED] completed all of the onsite work, while [REDACTED] worked remotely to get the server online.⁸⁷ After [REDACTED] left Secaucus, New Jersey, to travel back to PRN's headquarters, all physical pieces of hardware had been installed except for an intrusion detection device [REDACTED] told the FBI that Equinix installed this device shortly after he left because the intrusion detection device was shipped later.⁸⁸

b6
b7C

(U//~~FOUO~~) On or around June 30, 2013, [REDACTED] began to remotely migrate all e-mail accounts from the Pagliano Server to the PRN Server.⁸⁹ During this migration period, the two server systems functioned together to ensure uninterrupted e-mail delivery to users.⁹⁰ After several days of migration, all e-mail accounts hosted on the presidentclinton.com, wjcoffice.com, and clintonemail.com domains were transferred to the PRN Server.⁹¹ At that point, PRN kept the Pagliano Server online to ensure e-mail was still being delivered; however, the Pagliano Server was no longer hosting e-mail services for the Clintons.⁹²

b6
b7C

^o (U//~~FOUO~~) A third PRN employee, [REDACTED] only handled a few tasks related to the administration of the server system until he left the company in the summer of 2015.

b6
b7C

^p (U//~~FOUO~~) The PRN Server consisted of the following equipment: a Dell PowerEdge R620 server hosting four virtual machines, including four separate virtual machines for Microsoft Exchange e-mail hosting, a BES for the management of BlackBerry devices, a domain controller to authenticate password requests, and an administrative server to manage the other three virtual machines, a Datto SIRIS 2000 to store onsite and remote backups of the server system, a CloudJacket device for intrusion prevention, two Dell switches, and two Fortinet Fortigate 80C firewalls.

^q (U//~~FOUO~~) The [REDACTED] domain was also added to the PRN Server at a later date.

(U//~~FOUO~~) As part of the PRN Server environment, [REDACTED] told the FBI that he configured a backup device from Connecticut-based company Datto, Inc. (Datto), a Datto SIRIS 2000,^r to take multiple snapshots of the server system daily, with a retention period of 60 days.⁹³ The backup device also made multiple copies of the Pagliano Server between June 24, 2013 and December 23, 2013.⁹⁴ At the Clintons' request, PRN only intended that the backup device store local copies of the backups.^{95,96} However, in August 2015, Datto informed PRN that, due to a technical oversight, the PRN Server was also backing up the server to Datto's secure cloud storage.^{97,98} After this notification, PRN instructed Datto to discontinue the secure cloud backups.^{99,100}

b6
b7C

(U//~~FOUO~~) [REDACTED] stated the Clintons originally requested that e-mail on the PRN Server be encrypted such that no one but the users could read the content.¹⁰¹ However, PRN ultimately did not configure the e-mail settings this way to allow system administrators to troubleshoot problems occurring within user accounts.¹⁰²

b6
b7C

(U//~~FOUO~~) PRN utilized an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) called CloudJacket from SECNAP Network Security.¹⁰³ The IDS/IPS device implemented by PRN had pre-configured settings that blocked or blacklisted certain e-mail traffic identified as potentially harmful and provided real-time monitoring, alerting, and incident response services.^{104,105} SECNAP personnel would receive notifications when certain activity on the network triggered an alert.¹⁰⁶ These notifications were reviewed by SECNAP personnel and, at times, additional follow-up was conducted with PRN in order to ascertain whether specific activity on the network was normal or anomalous.¹⁰⁷ Occasionally, SECNAP would send e-mail notifications to [REDACTED] prompting him to block certain IP addresses.¹⁰⁸ [REDACTED] described these notifications as normal and did not recall any serious security incident or intrusion attempt.¹⁰⁹ PRN also implemented two firewalls for additional protection of the network. [REDACTED] stated that he put two firewalls in place for redundancy in case one went down.¹¹⁰

b6
b7C

(U//~~FOUO~~) According to the FBI's forensic analysis of the server system, on December 3, 2013, Microsoft Exchange was uninstalled on the Pagliano Server.¹¹¹ The Pagliano Server remained in the same server cage at the Equinix datacenter in Secaucus, New Jersey, and a forensic review of the server, which was obtained in August 2015 via consent provided by Clinton through Williams & Connolly, indicated that it continued to be powered on and off multiple times before the FBI obtained it.¹¹² At the time of the FBI's acquisition of the Pagliano Server, Williams & Connolly did not advise the US Government (USG) of the existence of the additional equipment associated with the Pagliano Server, or that Clinton's clintonemail.com e-mails had been migrated to the successor PRN Server remaining at Equinix. The FBI's subsequent investigation identified this additional equipment and revealed the e-mail migration. As a result, on October 3, 2015, the FBI obtained, via consent provided by Clinton through Williams & Connolly, both the remaining Pagliano Server equipment and the PRN Server, which had remained operational and was hosting Clinton's personal e-mail account until it was disconnected and produced to the FBI.^{113,114,115,116}

^r (U) The Datto SIRIS 2000 is a device that provides back-up capability and data redundancy.

(U//~~FOUO~~) Investigation determined Clinton and Abedin began using new e-mail accounts on the domain hrcoffice.com in December 2014.¹¹⁷ [REDACTED]

[REDACTED]
[REDACTED]^{118,119} Abedin stated the clintonemail.com system was “going away” and, following the initiation of the new domain, Abedin did not have access to her clintonemail.com account.¹²⁰ [REDACTED]

b3
b6
b7C

[REDACTED]^{121,122} This is consistent with representations made by Williams & Connolly, which stated in a February 22, 2016 letter: “Secretary Clinton did not transfer her clintonemail.com e-mails for the time period January 21, 2009 through February 1, 2013 to her hrcoffice.com account ...”¹²³ The investigation found no evidence Clinton's hrcoffice.com account contained or contains potentially classified information or e-mails from her tenure as Secretary of State. The FBI has, therefore, not requested or obtained equipment associated with Clinton's hrcoffice.com account.

D. (U//~~FOUO~~) *Mobile Devices Associated with Clinton's E-mail Server Systems*

(U//~~FOUO~~) Clinton stated she used a personal e-mail address and personal BlackBerry for both personal and official business and this decision was made out of convenience.¹²⁴ Abedin recalled that at the start of Clinton's tenure, State advised personal e-mail accounts could not be linked to State mobile devices and, as a result, Clinton decided to use a personal device in order to avoid carrying multiple devices.¹²⁵ [REDACTED]

b3
b6
b7C

[REDACTED]¹²⁷ Cooper stated that he was aware of Clinton using a second mobile phone number.^{s,128} Cooper indicated Clinton usually carried a flip phone along with her BlackBerry because it was more comfortable for communication and Clinton was able to use her BlackBerry while talking on the flip phone.¹²⁹ Clinton believed 212 [REDACTED] was her primary BlackBerry phone number, and she did not recall using a flip phone during her tenure at State, only during her service in the Senate.^{t,130} Abedin and Mills advised they were unaware of Clinton ever using a cellular phone other than the BlackBerry.^{131,132}

b6
b7C

(U//~~FOUO~~) FBI investigation identified 13 total mobile devices, associated with her two known phone numbers, 212 [REDACTED] and 212 [REDACTED] which potentially were used to send e-mails using Clinton's clintonemail.com e-mail addresses.¹³³ Investigation determined Clinton used in succession 11 e-mail capable BlackBerry mobile devices associated with 212 [REDACTED] eight of which she used during her tenure as Secretary of State.¹³⁴ Investigation identified Clinton used two e-mail capable mobile devices associated with 212 [REDACTED] after her tenure.^{u,135} On

b6
b7C

^s (U//~~FOUO~~) During his interview with the FBI, Cooper was mistakenly shown “202 [REDACTED]” as the second phone number. Cooper recognized the phone number as Clinton's second number; however the correct phone number is 212 [REDACTED]

^t (U//~~FOUO~~) AT&T toll records associated with 212 [REDACTED] indicated the number was consistently used for phone calls in 2009 and then used sporadically through the duration of Clinton's tenure and the years following. Records also showed that no BlackBerry devices were associated with this phone number.

^u (U//~~FOUO~~) The FBI identified four additional mobile devices associated with 212 [REDACTED] which were used during Clinton's tenure. However, these devices lacked e-mail capability, and as a result the FBI did not conduct any further investigation regarding these devices.

b6
b7C

February 9, 2016, DOJ requested all 13 mobile devices from Williams & Connolly.¹³⁶ Williams & Connolly replied on February 22, 2016 that they were unable to locate any of these devices.¹³⁷ As a result, the FBI was unable to acquire or forensically examine any of these 13 mobile devices.

(U//~~FOUO~~) On October 16, 2015, Williams & Connolly provided two other BlackBerry devices to the FBI and indicated the devices might contain or have previously contained e-mails from Clinton's personal e-mail account during her tenure as Secretary of State.^{v,138,139} FBI forensic analysis found no evidence to indicate either of the devices provided by Williams & Connolly were connected to one of Clinton's personal servers or contained e-mails from her personal accounts during her tenure.^{140,141,142}

(U//~~FOUO~~) The FBI identified five iPad devices associated with Clinton which potentially were used to send e-mails from Clinton's clintonemail.com e-mail addresses.^{143,144,145,146} The FBI obtained three of the iPads.^{147,148,149} One iPad contained three e-mails from 2012 in the hdr22@clintonemail.com "drafts" folder.¹⁵⁰ The FBI assessed the three e-mails did not contain potentially classified information.¹⁵¹ The FBI did not recover e-mails from Clinton's personal e-mail accounts from either of the other two iPads in its possession.¹⁵²

(U//~~FOUO~~) Monica Hanley, a former Clinton aide, often purchased replacement BlackBerry devices for Clinton during her tenure at State.¹⁵³ Hanley recalled purchasing most of the BlackBerry devices for Clinton from AT&T stores located in the Washington, D.C. area.¹⁵⁴ Whenever Clinton acquired new mobile devices, Cooper was usually responsible for setting up the new devices and syncing them to the server.¹⁵⁵ Abedin, and Hanley also assisted Clinton with setting up any new devices.¹⁵⁶ According to Abedin, it was not uncommon for Clinton to use a new BlackBerry for a few days and then immediately switch it out for an older version with which she was more familiar.¹⁵⁷ Clinton stated that when her BlackBerry device malfunctioned, her aides would assist her in obtaining a new BlackBerry, and, after moving to a new device, her old SIM cards were disposed of by her aides.¹⁵⁸ Cooper advised he sometimes assisted users, including Clinton, when they obtained a new mobile device by helping them back up the data from the old device before transferring it to the new device and syncing the new device with Clinton's server.¹⁵⁹ Abedin and Hanley indicated the whereabouts of Clinton's devices would frequently become unknown once she transitioned to a new device.^{160,161} Cooper did recall two instances where he destroyed Clinton's old mobile devices by breaking them in half or hitting them with a hammer.¹⁶²

b6
b7C

2. (U//~~FOUO~~) Clinton's Handling of E-mail and Classified Information

A. (U//~~FOUO~~) Clinton's Decision To Use Personal E-mail and Server Systems

(U//~~FOUO~~) FBI investigation determined the State Executive Secretariat's Office of Information Resource Management (S/ES-IRM) offered Clinton a State e-mail address at the start of her

^v (U//~~FOUO~~) The mobile devices provided to the FBI from Williams & Connolly on October 16, 2015 did not contain SIM cards or Secure Digital (SD) cards.

tenure; however, Clinton's staff^w declined the offer.¹⁶³ According to [redacted] State S/ES-IRM, Clinton was offered a State e-mail address, but instead decided to use the personal server from her 2008 presidential campaign.^{x,164} Investigation identified the existence of two State-issued e-mail accounts associated with Clinton; however, these accounts were used on Clinton's behalf and not by Clinton herself. According to State, SMSGs@state.gov was used to send e-mail messages from the Secretary to all State employees.^{165,166} This account was not configured to receive e-mails, and S/ES-IRM authored the messages sent from this account.¹⁶⁷ S/ES-IRM created SSHRC@state.gov to manage an Outlook calendar for Clinton, but this account was not configured to send or receive e-mails other than calendar invitations.^{168,169} A May 25, 2016 report issued by the State Office of Inspector General (OIG)^y stated that, during Clinton's tenure as Secretary of State, the State Foreign Affairs Manual (FAM) required day-to-day operations at State be conducted using an authorized information system.¹⁷⁰ The OIG stated it found "no evidence" that Clinton sought approval to conduct State business via her personal e-mail account or private servers, despite her obligation to do so.¹⁷¹ Clinton told the FBI that she did not explicitly request permission from State to use a private server or e-mail address.¹⁷² According to the State OIG report, State employees alleged that John Bentel, then-Director of S/ES-IRM, discouraged employees from raising concerns about Clinton's use of personal e-mail.^{z,173} When interviewed by the FBI, Bentel denied that State employees raised concerns about Clinton's e-mail to him, that he discouraged employees from discussing it, or that he was aware during Clinton's tenure that she was using a personal e-mail account or server to conduct official State business.¹⁷⁴

b6
b7C

(U//~~FOUO~~) The FBI investigation determined some Clinton aides and senior-level State employees were aware Clinton used a personal e-mail address for State business during her tenure. Clinton told the FBI it was common knowledge at State that she had a private e-mail address because it was displayed to anyone with whom she exchanged e-mails.¹⁷⁵ However, some State employees interviewed by the FBI explained that e-mails from Clinton only contained the letter "H" in the sender field and did not display her e-mail address.^{176,177,178} The majority of the State employees interviewed by the FBI who were in e-mail contact with Clinton indicated they had no knowledge of the private server in her Chappaqua residence.^{179,180,181,182,183,184} Clinton's immediate aides, to include Mills, Abedin, Jacob Sullivan,^{aa} and [redacted] told the FBI they were unaware of the existence of the private server until after Clinton's tenure at State or when it became public knowledge.^{185,186,187,188}

b6
b7C

^w (U//~~FOUO~~) S/ES-IRM employees interviewed indicated they did not communicate directly with Clinton regarding this issue and could not specifically identify the members of Clinton's immediate staff with whom they spoke.

^x (U//~~FOUO~~) According to [redacted] part of his job at State was to maintain and support the infrastructure for the UNCLASSIFIED and SECRET networks for the Executive Secretariat.

b6
b7C

^y (U//~~FOUO~~) Independent of the FBI's investigation, in April 2015, the State OIG initiated its own investigation and review of records management policies and practices regarding the use of non-State communications systems during the tenure of five Secretaries of State, including Clinton. Portions of the State OIG's May 25, 2016 report relevant to the FBI's investigation are cited herein.

^z (U) According to the State OIG report, two State information management staff members approached the Director of the S/ES-IRM in 2010 with concerns they had about Clinton's use of a personal e-mail account and compliance with federal records requirements. According to one staff member, the Director stated that Clinton's personal system had been reviewed and approved by State legal staff. The Director allegedly told both staff members never to discuss Clinton's personal e-mail system again. OIG found no evidence that State legal staff reviewed or approved Clinton's personal e-mail system.

^{aa} (U) Sullivan served as the Deputy Chief of Staff and later the Director of Policy and Planning during Clinton's tenure as Secretary of State.

(U//~~FOUO~~) The FBI investigation indicated Clinton was aware her use of a personal device, e-mail account, and server did not negate her obligation to preserve federal records. On January 23, 2009, Clinton contacted former Secretary of State Colin Powell via e-mail to inquire about his use of a BlackBerry while he was Secretary of State (January 2001 to January 2005).^{bb,189} In his e-mail reply, Powell warned Clinton that if it became "public" that Clinton had a BlackBerry, and she used it to "do business," her e-mails could become "official record[s] and subject to the law."¹⁹⁰ Powell further advised Clinton, "Be very careful. I got around it all by not saying much and not using systems that captured the data."¹⁹¹ Clinton indicated to the FBI that she understood Powell's comments to mean any work-related communications would be government records, and she stated Powell's comments did not factor into her decision to use a personal e-mail account.¹⁹² In an e-mail to Mills on August 30, 2011, State Executive Secretary, Stephen Mull, cited a request from Clinton to replace her temporarily malfunctioning personal BlackBerry with a State-issued device.¹⁹³ Mull informed Mills that a State-issued replacement device for Clinton's personal BlackBerry would be subject to FOIA requests.¹⁹⁴ On that same day, Bentel sent a separate e-mail to Hanley, which was later forwarded to Abedin, stating that e-mails sent to a State e-mail address for Clinton would be "subject to FOIA searches."¹⁹⁵ A State-issued device was not ultimately issued to Clinton; in her FBI interview, Abedin stated she felt it did not make sense to temporarily issue Clinton a State BlackBerry because it would have required significant effort to transfer all of her e-mails and contacts to a device that she would have only used for a few days.¹⁹⁶ The Mull and Bentel e-mails to Mills and Hanley did not indicate that transferring e-mail and/or contacts from Clinton's clintonemail.com account would be necessary to issue her a State BlackBerry.^{197,198,199} Abedin stated she always assumed all of Clinton's communications, regardless of the account, would be subject to FOIA if they contained work-related material.²⁰⁰

(U//~~FOUO~~) While State policy during Clinton's tenure required that "day-to-day operations [at State] be conducted on [an authorized information system],"²⁰¹ according to the [REDACTED] the Bureau of Information Security Management, [REDACTED] there was no restriction on the use of personal email accounts for official business.²⁰² However, State employees were cautioned about security and records retention concerns regarding the use of personal e-mail. In 2011, a notice to all State employees was sent on Clinton's behalf, which recommended employees avoid conducting State business from personal e-mail accounts due to information security concerns.²⁰³ Clinton stated she did not recall this specific notice, and she did not recall receiving any guidance from State regarding e-mail policies outlined in the State FAM.²⁰⁴ Interviews with two State employees determined that State issued guidance which required employees who used personal e-mail accounts for State business to forward those work-related e-mails to their official State account for record-keeping purposes.^{205,206} Investigation determined that State used the State Messaging and Archive Retrieval Toolset (SMART), which allows employees to electronically tag e-mails to preserve a record copy.^{207,208,209} According to [REDACTED] then State's [REDACTED] SMART was developed to automate and streamline the process for archiving records.²¹⁰ According to the

b6
b7Cb6
b7C

^{bb} (U) According to the State OIG report, when Powell arrived at State in 2001, the official unclassified e-mail system in place only permitted communication among State employees; therefore, Powell requested the use of a private line for his America Online (AOL) e-mail account to communicate with individuals outside of State. Prior to Powell's tenure, State employees did not have Internet connectivity on their desktop computers. During Powell's tenure, State introduced unclassified desktop external e-mail capability on a system known as OpenNet.

State OIG Report, IRM introduced SMART throughout State in 2009; however, the Office of the Secretary elected not to use the SMART system to preserve e-mails, partly due to concerns that the system would “allow overly broad access to sensitive materials.”²¹¹ [redacted] told the FBI that representatives from the Executive Secretariat asked to be the last to receive the SMART rollout, and ultimately SMART was never rolled out to the Executive Secretariat Office.²¹² This left the “print and file” method as the only approved method by which the Office of the Secretary could preserve record e-mails.²¹³

(U//~~FOUO~~) Mills wrote in a letter to State, dated December 5, 2014, that it was Clinton's practice to e-mail State officials at their government e-mail accounts for official business, and, therefore, State already had records of Clinton's e-mails preserved within State recordkeeping systems.²¹⁴ Abedin also stated in her FBI interview that Clinton's staff believed relevant e-mails would be captured and preserved by State if any of the senders or recipients were using an official State e-mail account.²¹⁵ The State OIG stated in its report that this was not an appropriate method of preserving record e-mails, and Clinton should have preserved any record e-mails created and received on her personal account by printing and filing the e-mails in the Office of the Secretary.²¹⁶ State OIG also determined Clinton should have surrendered all e-mails relating to State business before leaving her post as Secretary of State.²¹⁷ Clinton stated that she received no instructions or direction regarding the preservation or production of records from State during the transition out of her role as Secretary of State in early 2013.²¹⁸ Furthermore, Clinton believed her work-related e-mails were captured by her practice of sending e-mails to State employees' official State e-mail accounts.²¹⁹

B. (U//~~FOUO~~) *Communications Equipment in Clinton's State Office and Residences*

(U//~~FOUO~~) Investigation determined Clinton did not have a computer in her State office, which was located in a Sensitive Compartmented Information Facility (SCIF) on the seventh floor of State headquarters, in an area often referred to as “Mahogany Row.”^{220,221,222} State Diplomatic Security Service (DS) instructed Clinton that because her office was in a SCIF, the use of mobile devices in her office was prohibited.²²³ Interviews of three former DS agents revealed Clinton stored her personal BlackBerry in a desk drawer in DS “Post 1,”^{cc} which was located within the SCIF on Mahogany Row.^{224,225,226} State personnel were not authorized to bring their mobile devices into Post 1, as it was located within the SCIF.²²⁷ According to Abedin, Clinton primarily used her personal BlackBerry or personal iPad for checking e-mails, and she left the SCIF to do so, often visiting State's eighth floor balcony.²²⁸ Former Assistant Secretary of State for DS Eric Boswell stated he never received any complaints about Clinton using her personal BlackBerry inside the SCIF.²²⁹

(S//~~OC/NF~~) [redacted]

[redacted] This decision was relayed to Clinton's executive staff via a memo titled “Use of Blackberries in Mahogany Row,” dated March 6, 2009.²³² Clinton stated to the FBI that she requested a secure BlackBerry while at State after hearing President Obama had one, but she

^{cc} (S//~~OC/NF~~) The DS security detachment maintained a Post, known as Post 1, located in the SCIF and directly outside of Clinton's office on Mahogany Row.

could not recall the reasons why State was unable to fulfill this request.^{dd,233} Early in Clinton's tenure at State, Clinton's executive staff also inquired about the possibility of the Secretary using an iPad to receive communications in her office; however, this request was also denied due to restrictions associated with the Secretary's office being in a SCIF.²³⁴ According to the State OIG report, in January 2009, in response to Clinton's desire to take her BlackBerry into secure areas, Mills discussed with S/ES-IRM officials and with the State Under Secretary for Management, Patrick Kennedy, alternative solutions which would allow Clinton to check e-mail from her desk.²³⁵ Setting up an Internet-connected, stand-alone computer was discussed as a viable solution; however, a stand-alone system was never set up.²³⁶

(U) ~~(S//OC/NF)~~ Investigation determined Clinton had access to a number of State-authorized secure means of telephonic communication in her residences and in her office at State.^{ee,237} At the start of Clinton's tenure, State installed a SCIF and secure communications equipment. [redacted]

b1
b3

(S) [redacted] in her residences in Washington, D.C. (Whitehaven residence) and Chappaqua.^{ff,gg,hhh,238,239,240,241,242} According to Abedin, Cooper, and [redacted] there were personally-owned desktop computers in the SCIFs in Whitehaven and Chappaqua.^{243,244,245} Conversely, Clinton stated to the FBI she did not have a computer of any kind in the SCIFs in her residences.²⁴⁶ According to Abedin and Clinton, Clinton did not use a computer, and she primarily used her BlackBerry or iPad for checking e-mails.

b6
b7C

C. (U//~~FOUO~~) *Individuals in Direct Communication with Clinton's Personal E-mail Address*

(U//~~FOUO~~) Investigation determined a limited number of individuals maintained direct e-mail contact with Clinton through her personal clintonemail.com e-mail account during her tenure at State. Thirteen individuals, consisting of State senior-level employees, work-related advisors, and State executive administrative staff, maintained direct e-mail contact with Clinton and individually e-mailed her between 100 and 1,000 times during her tenure.ⁱⁱ Abedin, Mills, and Sullivan, were most frequently in e-mail contact with Clinton and accounted for 68 percent of the e-mails sent directly to Clinton. In addition to sending Clinton messages they wrote, Abedin, Mills, and Sullivan reviewed e-mails they received from other State employees, USG contacts, and foreign government contacts, and if deemed appropriate they then forwarded the information

(U) ~~(S//OC/NF)~~ According to Clinton, her request for a State-issued secure BlackBerry was not out of concern for the sensitivity of the information on the device she was using at the time, rather she wanted the secure device to deal with future contingencies.

b1
b3

^{ee} (S//~~OC/NF~~) According to Abedin, Clinton's State office contained [redacted]

^{ff} (U//~~FOUO~~) According to Abedin, the SCIF door at the Whitehaven residence was not always locked, and Abedin, Hanley, and [redacted] had access to the SCIF.

b6
b7C

(U) ^{gg} (S//~~OC/NF~~) Investigation determined the Chappaqua SCIF was not always secured, and Abedin, Hanley, and [redacted] had routine access to the SCIF.

b6
b7C

^{hh} (S//~~OC/NF~~) On [redacted] State installed the following communications lines at the Whitehaven residence [redacted]

[redacted] State installed communications equipment at the Chappaqua residence similar to that at the Whitehaven residence. State finished installation of the SCIF in the Chappaqua residence in [redacted]

b1
b3

ⁱⁱ (U//~~FOUO~~) The statistics in this paragraph are based on the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, excluding Clinton's personal correspondence with family and close friends, as well as e-mails Clinton forwarded to herself.

to Clinton.^{247,248,249} Multiple State employees advised they considered e-mailing Abedin, Mills, and Sullivan the equivalent of e-mailing Clinton.^{250,251}

(U//~~FOUO~~) Investigation identified hundreds of e-mails sent by Abedin and other State staff to [redacted]@presidentclinton.com e-mail address requesting him to print documents for Clinton. Some of these e-mails were determined to contain information classified at the CONFIDENTIAL level.^{jj,252,253,254,255,256,257} [redacted] received a security clearance at the SECRET level on October 25, 2007 from the Department of Defense (DOD).²⁵⁸ Documentation retained by DOD and provided to the FBI did not indicate [redacted] security clearance was deactivated upon his retirement from the US Navy Reserves in September 2010.²⁵⁹

b6
b7C

D. (U//~~FOUO~~) *Clinton Staff's Use of Personal E-mail Accounts for Official Business*

(U//~~FOUO~~) Clinton's immediate staff, to include Mills, Sullivan, Abedin, [redacted] and Hanley, told the FBI in interviews that they predominantly used their State-provided OpenNet e-mail accounts to conduct official State business.^{260,261,262,263,264} Exceptions to this practice included instances when the State OpenNet e-mail system was down or when staff was traveling internationally and OpenNet was not readily accessible.^{265,266,267,268,269} The FBI's investigation confirmed that Clinton's immediate staff used their personal e-mail accounts in combination with their State-provided OpenNet e-mail accounts for official State business.^{kk}

b6
b7C

E. (U//~~FOUO~~) *Clinton's Use of Personal E-mail Accounts While Overseas*

(U//~~FOUO~~) FBI investigation and the State OIG report determined that State issued regular notices to staff during Clinton's tenure highlighting cybersecurity threats and advising that mobile devices must be configured to State security guidelines.^{270,271} Clinton and her immediate staff were notified of foreign travel risks and were warned that digital threats began immediately upon landing in a foreign country, since connection of a mobile device to a local network provides opportunities for foreign adversaries to intercept voice and e-mail transmissions.^{272,273} The State Mobile Communications (MC) Team was responsible for establishing secure mobile voice and data communications for Clinton and her team when they were traveling domestically and abroad.^{274,275} When the security climate required, the State MC was capable of [redacted]

b1
b3

[redacted] could be received and viewed by Clinton and/or her designated staff.^{276,277}

(S//~~OC/NF~~) Investigation determined that of the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, approximately [redacted] e-mails were sent or received by Clinton on her personal e-mail accounts while she was traveling outside the continental United States (OCONUS) on official State business.^{ll,278} [redacted]

b1
b3

^{jj} (U//~~FOUO~~) Investigation identified six e-mail chains forwarded to [redacted] that were determined from the State FOIA review to contain CONFIDENTIAL information. Five were forwarded by Abedin, and one was from Clinton.

^{kk} (U) See Section 3.C for discussion of classified e-mails contained in Clinton's staff's personal e-mail accounts.

^{ll} (U//~~FOUO~~) State listed Clinton's overseas travel by individual days, but did not provide additional information such as arrival and departure times. As a result, the FBI could not determine specifically which e-mails were sent while she was on the ground OCONUS versus in flight.

b6
b7C

(S)

[REDACTED] FBI investigation determined that hundreds of e-mails classified CONFIDENTIAL during the State FOIA process were sent or received by Clinton while she was OCONUS. Approximately [REDACTED] e-mails were sent or received by Clinton [REDACTED]. On [REDACTED] occasions while OCONUS, Clinton had direct e-mail contact with an e-mail address for President Barack Obama. Of the [REDACTED] e-mails between Clinton and President Obama, [REDACTED] were sent and received [REDACTED]. None of these [REDACTED] e-mails were determined to contain classified information. Clinton told the FBI that she received no particular guidance as to how she should use President Obama's e-mail address, and the e-mails sent while Clinton was [REDACTED] nm, 279

b1
b3

F. (U//~~FOUO~~) *Clinton's Production of E-mail in Response to FOIA and Other Requests*

(U//~~FOUO~~) The House Select Committee on Benghazi was established on May 8, 2014 and reached an agreement with State on July 23, 2014 regarding the production of records.²⁸⁰ State sent a formal request to former Secretaries of State on October 28, 2014, asking them to produce e-mails related to their government work.²⁸¹ After State requested that Clinton provide her e-mails,^{nm} Clinton asked her attorneys, David Kendall^{oo} and Mills, to oversee the process of providing Clinton's work-related e-mails to State.²⁸² Heather Samuelson,^{pp} an attorney working with Mills, undertook a review to identify work-related e-mails, while Kendall and Mills oversaw the process.²⁸³ Ultimately, on December 5, 2014, Williams & Connolly provided approximately 55,000 pages of e-mails^{qq} to State in response to State's request for Clinton to produce all e-mail in her possession that constituted a federal record from her tenure as Secretary of State.²⁸⁴ State ultimately reviewed the 55,000 pages of e-mail to meet its production obligations related to FOIA lawsuits and requests. On May 27, 2015, State received a court order to post Clinton's e-mails to the State FOIA website on a monthly production schedule with a completion date of January 29, 2016.²⁸⁵ State ultimately concluded its FOIA-related production on February 29, 2016. Clinton told the FBI that she directed her legal team to provide any work-related or arguably work-related e-mails to State; however she did not participate in the development of the specific process to be used or in discussions of the locations of where her e-mails might exist.²⁸⁶ Clinton was not consulted on specific e-mails in order to determine if they were work-related.²⁸⁷

mm (S//~~OC/NF~~) [REDACTED]b1
b3

^{nm} (U//~~FOUO~~) During the summer of 2014, State indicated to Mills a request for Clinton's work-related e-mails would be forthcoming, and in October 2014, State followed up by sending an official request to Clinton asking for her work-related e-mails.

^{oo} (U) Kendall is a partner at Williams & Connolly.

^{pp} (U) Samuelson worked in the White House Liaison Office at State during Clinton's tenure and currently serves as Clinton's personal attorney.

^{qq} (U//~~FOUO~~) According to Clinton's campaign website, 30,490 potentially work-related e-mails were provided to State on December 5, 2014. On August 6, 2015, Williams & Connolly provided the FBI a .PST file containing 30,542 e-mail related files, which included 30,524 e-mail messages.

(U//~~FOUO~~) In July 2014, to initiate the review of Clinton's e-mails for production to State, Mills arranged for [REDACTED] to export from the PRN Server all of Clinton's e-mails sent to or received from a .gov e-mail address during Clinton's tenure as Secretary of State.^{288,289,290} Once [REDACTED] completed this export from the PRN Server, he remotely transferred a .PST file containing the e-mails onto Mills's and Samuelson's laptops via ScreenConnect.^{rr,291,292,293} In late September 2014, Mills and Samuelson asked [REDACTED] to provide a full export of all of Clinton's e-mails from her tenure, to include e-mails sent to and received from non-.gov e-mail addresses.^{294,295,296} Mills and Samuelson explained that this follow-up request was made to ensure their review captured all of the relevant e-mails from Clinton's tenure.^{297,298} [REDACTED] completed this export and transfer in the same manner as the July 2014 request.^{ss} Mills and Samuelson did not know from what location on the server [REDACTED] extracted Clinton's e-mails.^{299,300} [REDACTED] gave the FBI inconsistent statements over the course of three interviews regarding from where on the server he extracted Clinton's e-mails, and FBI investigation and forensic analysis have been unable to specifically identify the location and composition of the repository [REDACTED] used to create the export of Clinton's e-mails from her tenure.^{301,302,303}

b6
b7C

(U//~~FOUO~~) The FBI interviewed Samuelson on May 24, 2016 about her review of the PRN-provided e-mails. Samuelson indicated she conducted the review of these e-mails over the course of several months and completed it just prior to December 5, 2014, when hard copies of the work-related e-mails were turned over to State.³⁰⁴ Using her laptop to conduct the review, Samuelson placed any work-related e-mails into a folder that she had created in Microsoft Outlook.³⁰⁵ Samuelson first added to this folder all e-mails sent to or from Clinton's personal e-mail account with .gov and .mil e-mail addresses.³⁰⁶ Samuelson then searched the remaining e-mails for the names of State senior leadership, as well as any members of Congress, foreign leaders, or other official contacts.³⁰⁷ Finally, Samuelson conducted a key word search of terms such as "Afghanistan," "Libya," and "Benghazi."^{tt,308} Samuelson reviewed the "To," "From," and "Subject" fields of every e-mail during this review; however, she did not read the content of each individual e-mail, indicating that, in some instances, she made a determination as to whether it was one of Clinton's work or personal e-mails by only reviewing the "To," "From," and "Subject" fields of the e-mail.³⁰⁹

(U//~~FOUO~~) As she completed the review, Samuelson printed all of the e-mails to be turned over to State using a printer in Mills's office.³¹⁰ According to Samuelson, Mills and Kendall subsequently reviewed e-mails that Samuelson printed, and any hard copy of an e-mail Mills and Kendall deemed not to be work-related was shredded, and the digital copy of the e-mail was not included in the folder Samuelson created in Microsoft Outlook to contain all of the work-related e-mails.³¹¹ Mills stated that, other than instances where Samuelson requested Mills's guidance, Mills did not review the e-mails Samuelson identified as work-related, and once the review was complete, Samuelson printed the work-related e-mails.³¹² After the review was completed, Samuelson created a .PST file containing all of the work-related e-mails and ensured that all work-related e-mails were printed.³¹³ This .PST file was provided to Kendall on a USB thumb

^{rr} (U) ScreenConnect is a remote support administration tool that allows technicians to remotely connect to customers via a central web application to control and view end users' machines. According to product specifications, ScreenConnect encrypts data transmitted from one machine to another, to include screen data, file transfers, key strokes, and chat messages.

^{ss} (U//~~FOUO~~) Mills did not recall if this second .PST file was transferred to her computer.

^{tt} (U//~~FOUO~~) The FBI was unable to obtain a complete list of keywords or named officials searched from Samuelson, Mills, or Clinton's other attorneys due to an assertion of privilege.

drive.³¹⁴ On August 6, 2015, this thumb drive was obtained by the FBI from Williams & Connolly via consent from Clinton.

G. (U//~~FOUO~~) *Deletion of E-mail Associated with Clinton's Personal E-mail Accounts*

(U//~~FOUO~~) According to Hanley, in spring 2013, Cooper assisted Hanley in creating an archive of Clinton's e-mails.³¹⁵ Cooper provided Hanley with an Apple MacBook laptop (the Archive Laptop)^{uu} from the Clinton Foundation and telephonically walked Hanley through the process of remotely transferring Clinton's e-mails from the Pagliano Server to the laptop and a thumb drive.³¹⁶ Hanley completed this task from her personal residence.³¹⁷ The two copies of the Clinton e-mail archive (one on the Archive Laptop and one on the thumb drive) were intended to be stored in Clinton's Chappaqua and Whitehaven residences; however, Hanley explained this did not occur as Hanley forgot to provide the Archive Laptop and the thumb drive to Clinton's staff following the creation of the archive.^{318,319} In early 2014, Hanley located the Archive Laptop at her personal residence and worked with [REDACTED] to transfer the archive of Clinton's e-mails to PRN.^{320,321,322,323} After trying unsuccessfully to remotely transfer the e-mails to [REDACTED]

b6
b7C

[REDACTED] Hanley shipped the Archive Laptop to [REDACTED] residence in [REDACTED] in February 2014, and [REDACTED] migrated Clinton's e-mails from the Archive Laptop onto the PRN Server.^{324,325,326,327,328} To accomplish this, [REDACTED] transferred all of the Clinton e-mail content to a personal Google e-mail (Gmail) address he created, [REDACTED]@gmail.com, and then downloaded all of the e-mail content from the Gmail account to a mailbox named "HRC Archive" with the e-mail address hrcarchive@clintonemail.com on the PRN Server.^{329,330,331}

[REDACTED] advised he used the [REDACTED]@gmail.com e-mail account to facilitate the transfer because he had trouble exporting the e-mail from the Apple MacMail format to a format that would be compatible with Microsoft Exchange.³³²

(U//~~FOUO~~) Hanley stated she recommended that PRN wipe the Archive Laptop after the e-mails were transferred to the PRN Server.³³³ However, [REDACTED] told the FBI that, after the transfer was complete, he deleted the e-mails from the Archive Laptop but did not wipe the laptop.³³⁴ He also advised he deleted the e-mails uploaded to the [REDACTED]@gmail.com e-mail account per Hanley's instructions and shipped the Archive Laptop via United States Postal Service or United Parcel Service to [REDACTED] who was Clinton's [REDACTED] at the time.^{335,336,337} [REDACTED] told the FBI that she never received the laptop from [REDACTED] however, she advised that Clinton's staff was moving offices at the time, and it would have been easy for the package to get lost during the transition period.³³⁸ Neither Hanley nor [REDACTED] could identify the current whereabouts of the Archive Laptop or thumb drive containing the archive, and the FBI does not have either item in its possession.³³⁹

b6
b7C

(U//~~FOUO~~) FBI investigation identified 940 e-mails associated with Clinton's personal e-mail account from October 25, 2010 to December 31, 2010 that as of June 21, 2016 remained within the [REDACTED]@gmail.com account.³⁴⁰ The FBI was able to determine that 56 of these

b6
b7C

^{uu} (U//~~FOUO~~) According to Abedin, the archive of Clinton's e-mails was created as a reference for the future production of a book. According to Hanley, the archive of Clinton's e-mails was created in response to Clinton's hdr22@clintonemail.com address being released to the public following the online posting of e-mail exchanges between Clinton and an informal political advisor, Sidney Blumenthal. Blumenthal's personal e-mail account, which contained his e-mails with Clinton, was compromised on March 14, 2013 by a Romanian cyber hacker. See Section 4.D.

e-mails have been identified as currently classified at the CONFIDENTIAL level through the State FOIA process.³⁴¹ Additionally, the FBI determined that 302 of the 940 e-mails identified in the [redacted]@gmail.com account were not found in the set of e-mails Clinton produced to State in December 2014.³⁴² Of the 302 e-mails, the FBI disseminated 18 to USG agencies for classification review. State determined one e-mail to be classified SECRET when sent and to be classified CONFIDENTIAL currently. State determined a second e-mail to be classified as CONFIDENTIAL when sent and to be currently UNCLASSIFIED.

b6
b7C

(U//~~FOUO~~) In or around December 2014 or January 2015, Mills and Samuelson requested that [redacted] remove from their laptops all of the e-mails from the July and September 2014 exports.^{343,344,345} [redacted] used a program called BleachBit^{vv} to delete the e-mail-related files so they could not be recovered.^{346,347,348} [redacted] remotely connected to Mills's and Samuelson's laptops via ScreenConnect to complete the deletions.^{349,350,351} [redacted] stated to the FBI that an unknown Clinton staff member told him s/he did not want the .PST file after the export and wanted it removed from the PRN Server.³⁵² According to Mills, in December 2014, Clinton decided she no longer needed access to any of her e-mails older than 60 days.³⁵³ Therefore, Mills instructed [redacted] to modify the e-mail retention policy on Clinton's clintonemail.com e-mail account to reflect this change.³⁵⁴ However, according to [redacted] he did not make these changes to Clinton's clintonemail.com account until March 2015.³⁵⁵ Clinton told the FBI that, after her staff completed her e-mail production to State in December 2014, she was asked what she wanted to do with her remaining personal e-mails, Clinton instructed her staff she no longer needed the e-mails.³⁵⁶ Clinton stated she never deleted, nor did she instruct anyone to delete, her e-mails to avoid complying with FOIA, State or FBI requests for information.³⁵⁷

b6
b7C

(U//~~FOUO~~) On March 2, 2015, *The New York Times* (NYT) published an article titled, "Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules."^{ww,358} This article identified publicly that Clinton exclusively used a personal e-mail account to conduct official State business while she was Secretary of State and had not produced her federal records to State until December 2014.³⁵⁹ On March 3, 2015, the United States House Select Committee on Benghazi provided a letter to Williams & Connolly requesting the preservation and production of all documents and media related to hdr22@clintonemail.com and hrc17@clintonemail.com.^{xx,360} The following day, the House Select Committee on Benghazi issued a subpoena to Clinton to produce e-mails from hdr22@clintonemail.com, hrod17@clintonemail.com, and other e-mail addresses used by Clinton, pursuant to the events surrounding the 2012 terrorist attack in Benghazi.³⁶¹

(U//~~FOUO~~) In the days following the publication of the NYT article, Mills requested that PRN conduct a complete inventory of all equipment related to the Pagliano Server.^{362,363} In response to this request, [redacted] traveled to the Equinix datacenter in Secaucus, New Jersey to conduct an onsite review of the equipment, while [redacted] also logged in to the server

b6
b7C

^{vv} (U) BleachBit is open source software that allows users to "shred" files, clear Internet history, delete system and temporary files and wipe free space on a hard drive. Free space is the area of the hard drive that can contain data that has been deleted. BleachBit's "shred files" function claims to securely erase files by overwriting data to make the data unrecoverable.

^{ww} (U) The same article was released on the NYT website on March 2, 2015. The print version appeared on page A1 the following day, March 3, 2015.

^{xx} (U) The House Select Committee on Benghazi submitted a preservation request for an accurate e-mail address, hdr22@clintonemail.com, and an inaccurate e-mail address, hrc17@clintonemail.com, for Clinton.

remotely.^{364,365,366} [] powered on the Pagliano Server and confirmed for Mills that no additional data existed on any server equipment, as all data was migrated to the PRN Server.^{yy,367,368}

b6
b7C

(U//~~FOUO~~) Investigation indicated that on March 25, 2015, PRN held a conference call with President Clinton's staff.^{369,370} In his interviews with the FBI, [] indicated that sometime between March 25-31, 2015, he realized he did not make the e-mail retention policy changes to Clinton's clintonemail.com e-mail account that Mills had requested in December 2014.³⁷¹ In his FBI interview on February 18, 2016, [] indicated that he did not recall conducting deletions based upon this realization.³⁷² In a follow-up FBI interview on May 3, 2016, [] indicated he believed he had an "oh shit" moment and sometime between March 25-31, 2015 deleted the Clinton archive mailbox from the PRN server and used BleachBit to delete the exported .PST files he had created on the server system containing Clinton's e-mails.³⁷³ Investigation found evidence of these deletions³⁷⁴ and determined the Datto backups of the PRN Server were also manually deleted during this timeframe.³⁷⁵ Investigation identified a PRN work ticket, which referenced a conference call among PRN, Kendall, and Mills on March 31, 2015.^{376,377} PRN's attorney advised [] not to comment on the conversation with Kendall based upon the assertion of the attorney-client privilege.³⁷⁸

b6
b7C

(U//~~FOUO~~) Investigation identified a March 9, 2015 e-mail to PRN from Mills, of which [] was a recipient, referencing the preservation request from the Committee on Benghazi.^{379,380} [] advised during his February 18, 2016 interview that he did not recall seeing the preservation request referenced in the March 9, 2015 e-mail.³⁸¹ During his May 3, 2016 interview, [] indicated that, at the time he made the deletions in March 2015, he was aware of the existence of the preservation request and the fact that it meant he should not disturb Clinton's e-mail data on the PRN Server.³⁸² [] also stated during this interview, he did not receive guidance from other PRN personnel, PRN's legal counsel, or others regarding the meaning of the preservation request.³⁸³ Mills stated she was unaware that [] had conducted these deletions and modifications in March 2015.³⁸⁴ Clinton stated she was also unaware of the March 2015 e-mail deletions by PRN.³⁸⁵

b6
b7C

3. (U//~~FOUO~~) Results of FBI Review of Clinton E-mails Stored and Transmitted on Personal Server Systems

A. (U//~~FOUO~~) Quantities of Clinton's E-mails Recovered from Personal Server Systems

(U//~~FOUO~~) To date, the FBI has recovered from additional data sources and reviewed approximately 17,448 unique work-related and personal e-mails^{zz} from Clinton's tenure containing Clinton's hdr22@clintonemail.com^{aaa} e-mail address that were not provided by

^{yy} (U//~~FOUO~~) FBI forensically identified deletions from the PRN Server on March 8, 2015 of .PST files not associated with Clinton's e-mail account or domain, and other server data.

^{zz} (U//~~FOUO~~) These approximately 17,448 e-mails were determined to be unique from the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, through a distinctive Internet Message ID. These files do not include documents or partial e-mail files without an Internet Message ID in the metadata.

^{aaa} (U//~~FOUO~~) The approximate 17,448 e-mails may contain chains of e-mails in which Clinton is not on the most recent "To," "From," "CC," or "BCC" line.

Williams & Connolly as part of Clinton's production to the FBI, including e-mails from January 23, 2009 through March 18, 2009.^{bbb}

B. (U//~~FOUO~~) Classification Portion Markings in E-mail Recovered from Personal Server Systems

(U//~~FOUO~~) The FBI identified three e-mail chains, encompassing eight individual e-mail exchanges to or from Clinton's personal e-mail accounts, which contained at least one paragraph marked "(C)," a marking ostensibly indicating the presence of information classified at the CONFIDENTIAL level.^{386,387,388} The emails contained no additional markings, such as a header or footer, indicating that they were classified. State confirmed through the FOIA review process that one of these three e-mail chains contains information which is currently classified at the CONFIDENTIAL level.^{ccc,389} State determined that the other two e-mail chains are currently UNCLASSIFIED.^{390,391} State did not provide a determination as to whether any of these three e-mails were classified at the time they were sent.

(U//~~FOUO~~) When asked about the e-mail chain containing "(C)" portion markings that State determined to currently contain CONFIDENTIAL information, Clinton stated she did not know what the "(C)" meant at the beginning of the paragraphs and speculated it was referencing paragraphs marked in alphabetical order.^{ddd,392} Clinton identified a "CONFIDENTIAL" header and footer (inserted in the document by the FBI prior to the interview) and asked if the "(C)" related to the "CONFIDENTIAL" header and footer.³⁹³ Clinton did not believe the content of the e-mail was classified and questioned the classification determination.³⁹⁴ When asked of her knowledge regarding TOP SECRET, SECRET, and CONFIDENTIAL classification levels of USG information, Clinton responded that she did not pay attention to the "level" of classification and took all classified information seriously.³⁹⁵

C. (U//~~FOUO~~) Classified Information Found in Clinton's E-mails on Personal Server Systems

(U//~~FOUO~~) FBI and USIC classification reviews identified 81 e-mail chains containing approximately 193 individual e-mail exchanges^{eee} that were classified from the CONFIDENTIAL to TOP SECRET levels at the time the e-mails were drafted on UNCLASSIFIED systems and sent to or from Clinton's personal server. Of the 81 e-mail chains classified at the time of transmittal, 68 remain classified. Twelve of the e-mail chains, classified

^{bbb} (U//~~FOUO~~) According to Clinton's campaign website, Clinton only provided State her work-related e-mails dated after March 18, 2009. E-mails from January 21, 2009 to March 18, 2009 were not produced to State or the FBI by Williams & Connolly. According to Samuelson and Mills, they were unable to locate Clinton's e-mails from this period. The e-mails from this time period were not provided to them by PRN, and they believed the e-mails were not backed up on any server. Investigation determined some of Clinton's e-mails from January 23, 2009 to March 17, 2009 were captured through a Datto backup on June 29, 2013. However, the e-mails obtained are likely only a subset of the e-mails sent or received by Clinton during this time period.

^{ccc} (U//~~FOUO~~) The three e-mail chains containing the portion mark of "(C)" are not considered as part of the group of e-mails classified through the FBI classification review because State has not responded to the FBI request for classification determinations for these e-mails.

^{ddd} (U//~~FOUO~~) Earlier in her FBI interview, when asked what the classification marking "(SBU)" meant, Clinton correctly stated Sensitive But Unclassified.

^{eee} (U//~~FOUO~~) Due to the limited insight into other USG and personal e-mail accounts, the investigation was unable to determine if e-mails from the classified e-mail chains were forwarded to other USG or personal e-mail addresses.

by State as SECRET or CONFIDENTIAL, were not among the approximately 30,000 e-mails provided to State and the FBI by Williams & Connolly. In addition to State classified equities, the investigation determined the 81 e-mail chains contained classified equities from 5 other USIC agencies: the CIA, DOD, FBI, National Geospatial–Intelligence Agency (NGA), and National Security Agency (NSA).

(S//~~OC/NF~~) The 81 classified e-mail chains contained 8 e-mail chains classified TOP SECRET, 37 e-mail chains classified SECRET, and 36 e-mail chains classified CONFIDENTIAL at the time they were sent. Of these e-mail chains, 7 e-mail chains contained information associated with a Special Access Program (SAP) and 3 e-mail chains contained Sensitive Compartmented Information (SCI).^{fff} Of the 81 classified e-mail chains, 36 e-mail chains were determined to be Not-Releasable to Foreign Governments (NOFORN) and 2 were considered releasable only to Five Allied partners (FVEY). []

b1
b3

[]
Sixteen of the e-mail chains, classified at the time the e-mails were sent, were downgraded in current classification by USIC agencies.

(S//~~OC/NF~~) []
[]

- (S//~~OC/NF~~) []
- (S//~~OC/NF~~) []
- (S//~~OC/NF~~) []
- (S//~~OC/NF~~) []
[]
- (S//~~OC/NF~~) []
[]
- (S//~~OC/NF~~) []
[]
- (S//~~OC/NF~~) []
- (S//~~OC/NF~~) []
[]

b1
b3

(U//~~FOUO~~) The State FOIA process identified 2,093 e-mails currently classified as CONFIDENTIAL or SECRET. Of these e-mails, FBI investigation identified approximately 100 e-mails that overlapped with the 193 e-mails (80 e-mail chains) determined through the FBI

^{fff} (U//~~FOUO~~) One of the TOP SECRET/SCI e-mails was downgraded to a current classification of SECRET//REL TO USA, FVEY by the owning agency during a FOIA-related review.

classification review to be classified at the time sent. All except one of the remaining 2,093 e-mails were determined by the State FOIA process to be CONFIDENTIAL, with one e-mail determined to be SECRET at the time of the FOIA review.^{ggg, hhh} State did not provide a determination as to whether the 2,093 e-mails were classified at the time they were sent.

(U//~~FOUO~~) The FBI investigation determined Clinton contributed to discussions in four e-mail chains classified as CONFIDENTIAL, three e-mail chains classified as SECRET//NOFORN, and four e-mail chains classified as TOP SECRET/SAP. Investigation identified 67 instances where Clinton forwarded e-mails to either State personnel or [redacted] for printing that were identified as classified CONFIDENTIAL or SECRET through either the State FOIA process or FBI classification determination requests.

b6
b7C

(U//~~FOUO~~) FBI investigation determined at least 32 classified e-mail chains transited both the personal e-mail account of Clinton and the personal e-mail accounts of Abedin, Mills, Sullivan, or [redacted].ⁱⁱⁱ One of these e-mails was TOP SECRET/SCI at the time of transmission, and is currently considered SECRET//REL TO USA, FVEY; five were classified as SECRET//NOFORN and one as SECRET both when sent and currently; two were classified SECRET when sent and are CONFIDENTIAL currently; one was classified as SECRET when sent and is UNCLASSIFIED//FOUO currently; 16 were classified CONFIDENTIAL both when sent and currently; five were CONFIDENTIAL when sent and UNCLASSIFIED//FOUO currently; and one was CONFIDENTIAL when sent and UNCLASSIFIED currently.ⁱⁱⁱ Investigation determined at least 80 e-mails from the 2,093 e-mails deemed classified through the State FOIA process were sent to or from the personal accounts of Abedin, Mills, Sullivan, or [redacted].^{kk}

b6
b7C

D. (U//~~FOUO~~) Witness Statements Related to Classified E-mails Found on Clinton's Personal Server Systems

(U//~~FOUO~~) The FBI interviewed multiple officials who authored and/or contributed to e-mails, the content of which has since been determined to contain classified information.^{396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408} USG employees responsible for initiating classified e-mail chains included State Civil Service employees, Foreign Service employees, Senior Executive Service employees, Presidential appointees, and non-State elected officials.

(U//~~FOUO~~) During FBI interviews, the authors of these e-mails provided context surrounding the e-mails in question as well as reasons for sending the e-mails on unclassified systems.

^{ggg} (U//~~FOUO~~) Investigation determined the following types of e-mails were not included in the list of 2,093 e-mails classified through the State FOIA review: TS/SAP e-mails; e-mails not produced to State by Williams & Connolly; formerly classified e-mails now considered UNCLASSIFIED; and classified e-mails improperly released during FOIA production.

^{hhh} (U//~~FOUO~~) Two attachments labeled as SECRET through State FOIA process were not tracked as separate classified documents in the FBI's classification review.

ⁱⁱⁱ (U//~~FOUO~~) Due to the limited insight into other USG and personal e-mail accounts, FBI investigation was unable to determine if e-mails from classified e-mail chains were forwarded to other personal e-mail accounts.

ⁱⁱⁱ (U//~~FOUO~~) In addition to the personal accounts of Abedin, Mills, Sullivan, and [redacted] seven classified e-mail chains were initially drafted in or sent from the private e-mail accounts of five non-State individuals, to include Kerry and Blumenthal.

^{kkk} (U//~~FOUO~~) Personal e-mail accounts of Abedin, Mills, Sullivan, and [redacted] appeared in the "To," "From," or "CC" line of the e-mail. Investigation was not able to determine if additional personal accounts were blind carbon copied ("BCC").

b6
b7C

Individuals who worked in the State Bureau of Public Affairs^{III} often accessed classified information to understand the context of unclassified information that was to be disseminated publicly.⁴⁰⁹ The Public Affairs officials primarily relied upon reporting from country desk officers to generate talking points and believed the country desk officers were experienced in protecting sensitive information within their reporting.⁴¹⁰ The Public Affairs officials were also responsible for notifying State leadership of impending reports by the news media regarding sensitive or controversial topics.⁴¹¹ Furthermore, a former DOD official explained that he sent an e-mail, since deemed to contain classified information, in order to quickly coordinate public affairs responses by State and DOD with respect to a specific incident referenced in the e-mail.⁴¹²

(U//~~FOUO~~) Individuals, including those in the State Operations Center (Ops Center),^{mmmm} who were responsible for passing information to high-level State officials, worked to identify and disseminate the information they deemed critical for review by State leadership.^{413,414} These individuals noted that such information was generally sent on State unclassified e-mail systems because of the need to quickly elevate information at times when the intended recipients did not all have immediate access to classified e-mail accounts.^{nnn,415,416}

(U//~~FOUO~~) Investigation identified seven e-mail chains comprised of 22 e-mails on Clinton's server classified by the USIC as TOP SECRET/SAP. State Department officials, both in Washington, D.C. and overseas, were briefed into the SAP and communicated both internally and with other USIC officials about the program.^{417,418,419,420} Only internal State e-mails regarding the SAP were forwarded to Clinton, all of which were sent to Clinton's server by Sullivan. Clinton and Sullivan engaged in discussions regarding the SAP in four of the seven e-mail chains.

(S//~~OC/NF~~) During FBI interviews, State employees explained the context for why classified material [REDACTED] was sent and provided reasons to explain why they did not believe information in the e-mails was classified.^{421,422,423,424} [REDACTED]

[REDACTED] stated that [REDACTED]

b1
b3
b6
b7C

[REDACTED]⁴²⁷ [REDACTED] stated the right method of communication was whichever method allowed for the fastest possible dissemination of the message.⁴²⁸ He also stated that information he received from other USG agencies was "technically probably classified" but that "you can't do business

^{III} (U//~~FOUO~~) According to State's website, the Bureau of Public Affairs "engages domestic and international media to communicate timely and accurate information with the goal of furthering US foreign policy and national security interests as well as broadening understanding of American values."

^{mmmm} (U//~~FOUO~~) The Ops Center is staffed 24 hours a day and constantly monitors reporting from State cables, other USG agencies, and open source news outlets for information of interest to State leadership.

ⁿⁿⁿ (U//~~FOUO~~) Individuals who inputted classified information into e-mail chains to pass to high-level State officials indicated that at times they were relying on information that others had summarized and provided to them.

that way.”⁴²⁹ When interviewed by the FBI, authors of the e-mails stated that they used their best judgment in drafting the messages and that it was common practice at State to carefully word e-mails on UNCLASSIFIED networks so as to avoid sensitive details or “talk around” [redacted] classified information.^{430,431,432,433} [redacted] stated the information in the [redacted]

b1
b3
b6
b7C

(S) [redacted] former [redacted] declined to comment on the e-mails.⁴³⁵ [redacted] referenced news articles claiming e-mails on Clinton's server were over-classified, but after seeing the e-mails during the interview, stated he “now understood why people were concerned about this matter.”⁴³⁶ Sullivan indicated he had no reason to believe any State employee ever intentionally mishandled classified information.⁴³⁷

(S//~~OC/NF~~) The FBI interviewed four USIC executives stationed both in the United States and overseas [redacted].^{438,439,440,441} The USIC executives reviewed the [redacted] e-mail chains which transited Clinton's personal e-mail account and assessed that some of the e-mail chains should be considered classified.^{442,443,444} [redacted]

b1
b3

[redacted]⁴⁴⁰ However, two of the USIC executives interviewed said some of the [redacted]


(S//~~OC/NF~~) A majority of the USIC executives interviewed expressed concerns with how State handled [redacted].^{449,450,451} According to a USIC executive who had been stationed overseas, State employees were aware of the sensitivities [redacted].⁴⁵² [redacted]

b1
b3

(U//~~FOUO~~) On April 9, 2016, Mills, who served as Chief of Staff to Clinton at State between 2009 and 2013, was interviewed by the FBI. During this interview, Mills was provided seven e-mails which contained information later determined to be classified. While Mills did not specifically remember any of the e-mails, she stated that there was nothing in them that concerned her regarding their transmission on an unclassified e-mail system.⁴⁵⁵ Mills also stated that she was not concerned about her decision to forward certain of these e-mails to Clinton.⁴⁵⁶ In reviewing e-mails related to the SAP referenced above, Mills explained that some of the e-mails were designed to inform State officials of media reports concerning the subject matter and that the information in the e-mails merely confirmed what the public already knew.⁴⁵⁷

(U//~~FOUO~~) The FBI interviewed Sullivan on February 27, 2016. Sullivan, who between 2009 and 2013 served at State first as the Deputy Chief of Staff for Policy and then as the Director of Policy Planning, communicated extensively with Clinton by e-mail. Their communications included both e-mails written by Sullivan and e-mails written by others that Sullivan forwarded to Clinton. During the interview, the FBI asked Sullivan to review approximately 14 e-mails Sullivan sent or received on unclassified systems that were later determined to contain classified information up to the TOP SECRET/SAP level. Sullivan did not specifically recall the e-mails, aside from recognizing some of them from the materials released pursuant to FOIA litigation, but

provided reasons why the e-mails may have been sent by him or others on unclassified systems.⁴⁵⁸ With respect to the SAP, Sullivan stated that it was discussed on unclassified systems due to the operational tempo at that time, and State employees attempted to talk around classified information.⁴⁵⁹ Sullivan also indicated that, for some of the e-mails, information about the incidents described therein may have already appeared in news reports.⁴⁶⁰ Furthermore, Sullivan stated that his colleagues at State worked hard while under pressure and used their best judgment to accomplish their mission.⁴⁶¹ When forwarding e-mails, Sullivan relied on the judgment of the individuals who sent the e-mails to him to ensure that the e-mails did not contain classified information.⁴⁶² Sullivan did not recall any instances in which he felt uneasy about information conveyed on unclassified systems, nor any instances in which others expressed concerns about the handling of classified information at State.^{ooo,463}

(S//~~OC/NF~~) Sullivan was also asked about an e-mail exchange between him and Clinton in which, on the morning of June 17, 2011, Clinton asked Sullivan to check on the status of talking points she was supposed to have received.⁴⁶⁴ Sullivan responded that the secure fax was malfunctioning but was in the process of being fixed. Clinton instructed Sullivan that if the secure fax could not be fixed, he should “turn [the talking points] into nonpaper [with] no identifying heading and send nonsecure.”⁴⁶⁵ State uses the term “non-paper” to refer to a document which is authorized for distribution to a foreign government without explicit attribution to the U.S. government and without classified information. Sullivan did not recall this specific e-mail but believed that Clinton's request indicated that she would have wanted him to make an unclassified version of the document, summarize the contents, and then send it to her on a non-secure fax.⁴⁶⁶ 

b1
b3

(U//~~FOUO~~) On April 5, 2016, Abedin, who served as Deputy Chief of Staff to Clinton at State between 2009 and 2013, was interviewed by the FBI. When asked about an e-mail subsequently determined to contain CONFIDENTIAL information, Abedin noted that she had only conveyed the information from the e-mail and had not originated it.⁴⁷⁰ She also stated that she relied upon the sender to properly mark the e-mail for classification purposes and did not take it upon herself to question the sender's judgment as to such marking.^{ppp,471}

(U//~~FOUO~~) Investigation determined Sidney Blumenthal, a former political aide to President Clinton and an informal political advisor to Clinton during her tenure at State, had direct e-mail contact with Clinton during her tenure at State. FBI investigation identified at least 179 e-

^{ooo} (U//~~FOUO~~) Abedin and Mills also provided similar responses when asked about State security practices regarding classified information.

^{ppp} (U//~~FOUO~~) Although Abedin was a party to e-mails containing information that has since been determined to be classified, due to the nature of her position at State, Abedin was not regularly included in the e-mail chains (discussed in this section of the memorandum) about which Sullivan and Mills were questioned. Abedin's position at State did not consistently involve her participation in substantive policy decisions, and she was not a regular user of classified e-mail systems.

mails^{qqq} that Blumenthal sent to Clinton containing information in memorandum format. The State FOIA process identified 24 memos from Blumenthal that contained information currently classified as CONFIDENTIAL and one as SECRET both when sent and currently.^{472,473} The FBI interviewed Blumenthal on January 7, 2016. According to Blumenthal, the content of the memos, which addressed topics to include Benghazi and foreign political developments, was provided to him from a number of different sources to include former USIC employees and contacts, as well as contacts within foreign governments.^{474,475,476,477,478,479,480,481,482,483,484,485,486,487} The memos contained a notation of "CONFIDENTIAL"^{trr} and then often included a source summary statement^{sss} similar to those frequently found in USIC intelligence products.^{488,489,490} Blumenthal indicated he was not tasked to provide this information to Clinton; rather, he provided it because he deemed the information helpful, which Clinton occasionally acknowledged via e-mail.⁴⁹¹ Clinton often forwarded the memos to Sullivan asking him to remove information identifying Blumenthal as the originator and to pass the information to other State employees to solicit their input.^{492,493} According to e-mails between Clinton and Sullivan, Clinton discussed passing the information to the White House, other USG agencies, and foreign governments.^{ttt,494,495}

E. (U//~~FOUO~~) Clinton's Statements Related to Classified E-mails Found on Her Personal Server Systems

(S//~~OC/NF~~) On July 2, 2016, the FBI interviewed Clinton. Clinton was aware she was an Original Classification Authority (OCA) at State; however, she could not recall how often she used this authority nor could she recall any training or guidance provided by State.⁴⁹⁶ Clinton could not give an example of how the classification of a document was determined; rather she stated there was a process in place at State before her tenure, and she relied on career foreign service professionals to appropriately mark and handle classified information.⁴⁹⁷ Clinton believed information should be classified when it relates to [redacted] the use of sensitive sources, or sensitive deliberations.⁴⁹⁸ When asked whether she believed information should be classified if its unauthorized release would cause damage to national security, Clinton responded "yes, that is the understanding."⁴⁹⁹

b1
b3

(U//~~S/OC/NF~~) Clinton did not recall receiving any e-mails she thought should not have been on an unclassified system.⁵⁰⁰ She relied on State officials to use their judgment when e-mailing her and could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her e-mail address.⁵⁰¹ The FBI provided Clinton with copies of her classified e-mails ranging from CONFIDENTIAL to TOP SECRET/SAP and Clinton said she did not believe the e-mails contained classified information.⁵⁰² Upon reviewing an e-mail classified SECRET//NOFORN dated December 27, 2011, Clinton stated no policy or practice existed

^{qqq} (U//~~FOUO~~) The FBI obtained 177 of Blumenthal's memos from the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI. The FBI recovered two additional memos during the investigation from BlackBerry backups provided by Cooper; State did not provide a classification determination on those additional memos.

^{trr} (U//~~FOUO~~) According to Blumenthal, "CONFIDENTIAL" meant the memo was personal in nature and did not refer to classified USG information.

^{sss} (U//~~FOUO~~) According to Blumenthal, the individual who provided the content for a number of the memos authored the source summary statements (caveats provided regarding the source of information) in the memos.

^{ttt} (U//~~FOUO~~) Investigation was unable to determine if any of Blumenthal's memos were forwarded to the White House, or to other USG agencies and foreign governments, as Sullivan's OpenNet sent items were not present in the data provided by State to the FBI.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

related to communicating around holidays, and it was often necessary to communicate in code or do the best you could to convey the information considering the e-mail system you were using.⁵⁰³ In reference to the same e-mail, Clinton believed if the foreign press was to obtain information from that e-mail, it would not cause damage to the US Government.⁵⁰⁴ When asked, Clinton recalled being briefed on SAP information but could not recall any specific briefing on how to handle SAP information.⁵⁰⁵ Clinton stated she knew SAP information was of great importance and needed to be handled carefully.⁵⁰⁶

F. (U//~~FOUO~~) Gaps in Clinton E-mail Recovered from Personal Server Systems

(U//~~FOUO~~) There were no e-mails provided by Williams & Connolly to State or the FBI dated from January 21, 2009 to March 18, 2009. FBI investigation identified an additional 18 days where Clinton did not provide State any responsive e-mail. FBI investigation determined 14 of the 18 days where Clinton did not provide State any responsive e-mail correspond with e-mail outages affecting Clinton's personal server systems as a result of both Hurricane Irene^{uuu} and Hurricane Sandy^{vvv}. FBI investigation indicated other explanations for gaps in Clinton's e-mail production could include user deletion prior to PRN's transfer of Clinton's e-mails for review, or flaws in the archiving and sorting process used to generate the responsive production to State.

4. (U//~~FOUO~~) Results of the FBI Investigation and Analysis of Cyber Intrusion Potential

A. (U//~~FOUO~~) Cyber Analysis of Clinton's Personal Server Systems

(U//~~FOUO~~) FBI investigation and forensic analysis did not find evidence confirming that Clinton's e-mail server systems were compromised by cyber means. The FBI's inability to recover all server equipment and the lack of complete server log data for the relevant time period limited the FBI's forensic analysis of the server systems. As a result, FBI cyber analysis relied, in large part, on witness statements, e-mail correspondence, and related forensic content found on other devices to understand the setup, maintenance, administration, and security of the server systems.

(U//~~FOUO~~) Investigation determined Clinton's clintonemail.com e-mail traffic was potentially vulnerable to compromise when she first began using her personal account in January 2009. It was not until late March 2009, when the Pagliano Server was set up and an SSL certificate^{www} was acquired for the clintonemail.com domain—providing encryption of login credentials, but not e-mail content stored on the server—that access to the server was afforded an added layer of security.^{507,508} The certificate was valid until September 13, 2013, at which time PRN obtained a new certificate valid until September 13, 2018.⁵⁰⁹

(U//~~FOUO~~) During his December 22, 2015 FBI interview, Pagliano recalled a conversation with [REDACTED] at the beginning of Clinton's tenure, in which [REDACTED] advised he would not be

b6
b7C

^{uuu} (U//~~FOUO~~) The first of two extended outages occurred from August 28 to 30, 2011 (3 days) as a result of Hurricane Irene.

^{vvv} (U//~~FOUO~~) The second extended outage occurred from October 30, 2012 to November 9, 2012 (11 days) as a result of Hurricane Sandy.

^{www} (U//~~FOUO~~) According to FBI forensic analysis, there was no SSL certificate on the Pagliano Server between March 19, 2009, when the mail service was operational, and March 29 or 30, 2009, when the SSL certificate was installed on the server.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

~~SECRET//ORCON/NOFORN~~ [REDACTED]

surprised if classified information was being transmitted to Clinton's personal server.⁵¹⁰ [REDACTED] further recommended that e-mail transiting from a state.gov account to the server should be sent through a Transport Layer Security (TLS)^{xxx} tunnel.^{yyy} Pagliano advised that the transition to TLS never occurred.^{511,512} The FBI was unable to forensically determine if TLS was implemented on the Pagliano Server.

b6
b7C

(U//~~FOUO~~) When asked about the maintenance and security of the server system he administered, Pagliano stated there were no security breaches, but he was aware there were many failed login attempts, which he referred to as brute force attacks.^{zzz,513} He added that the failed attempts increased over the life of the Pagliano Server, and he set up the server's logs to alert Cooper when they occurred.⁵¹⁴ Pagliano knew the attempts were potential attackers because the credentials attempting to log in did not match legitimate users on the system.⁵¹⁵ Pagliano could not recall if a high volume of failed login attempts emanated from any specific country.⁵¹⁶

(U//~~FOUO~~) In an attempt to thwart potential attacks, Pagliano set up Internet Protocol (IP) filtering^{aaaa} on the firewall and tried to review the firewall log files once a month.⁵¹⁷ After the Pagliano Server was established, Cooper put Pagliano in contact with [REDACTED] a United States Secret Service (USSS) agent, who recommended Pagliano also perform outbound filtering of e-mail traffic.⁵¹⁸ Pagliano further considered, but ultimately did not implement, a Virtual Private Network (VPN)^{bbbb} or two-factor authentication^{cccc} to better secure administrative access to the server system by him and Cooper.⁵¹⁹ The FBI forensically determined that Remote Desktop Protocol (RDP)^{dddd} was enabled on the Pagliano Server and was used by Pagliano, Cooper, and later PRN, for remote administration of the server.⁵²⁰ While the availability of RDP

b6
b7C

^{xxx} (U) TLS is a protocol that ensures privacy between communicating applications, such as web browsing, e-mail, and instant-messaging, with their users on the Internet. TLS ensures that no third-party eavesdrops on the two-way communication. TLS is the successor to SSL and is considered more secure.

^{yyy} (U) According to the State OIG report, State policy (12 FAM 544.3) stipulates normal day-to-day operations must be conducted on an authorized system. In the absence of a device, such as a State OpenNet terminal, employees can send most Sensitive But Unclassified (SBU) information unencrypted via the Internet only when necessary, with the knowledge that the nature of the transmission lends itself to unauthorized access, however remote that chance might be. Furthermore, in August 2008, 12 FAM 682.2-5 was amended and mandated that SBU information on non-Department-owned systems at non-Departmental facilities had to meet certain criteria. Employees had to: 1) ensure that SBU information was encrypted; 2) destroy SBU information on their personally owned and managed computers and removable media when the files are no longer required; and 3) implement encryption certified by the National Institute of Science and Technology (NIST), among other things. Although 12 FAM 682.2-5 was further amended in 2009, 2011, 2014, and 2015, the basic requirements did not change.

^{zzz} (U) A brute force attack is a trial-and-error method used to obtain information, such as a password or personal identification number (PIN). In a brute force attack, passwords may be attempted manually or automated software can be used to generate a large number of consecutive guesses as to the targeted information.

^{aaaa} (U) IP filtering is the practice of identifying and manually blocking IP addresses based on the identification of patterns that are indicative of a potential attack.

^{bbbb} (U) VPN is a private network that runs on top of a larger network to provide access to shared network resources, which may or may not include the physical hard drives of individual computers, as in the case of Remote Desktop Protocol (RDP). VPN offers an additional layer of security by encrypting the data traveling to the private network before sending it over the Internet. Data is then decrypted when it reaches the private network.

^{cccc} (U) Two-factor authentication is a method of confirming a user's claimed identity by utilizing a combination of two different components, often something the user knows and something the user has—such as a RSA keyfob/token.

^{dddd} (U) RDP is a proprietary protocol developed by Microsoft that allows a user to remotely connect to another computer over a network connection to view the computer and control it remotely. RDP is implemented in every version of Windows starting with Windows XP.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

on a server is convenient for remote access, the FBI is aware of known vulnerabilities^{eeee} associated with the protocol.

(U//~~FOUO~~) [redacted]

b3

[redacted]^{523,524} Pagliano recalled finding “a virus,” but could provide no additional details, other than it was nothing of great concern.⁵²⁵ FBI examination of the Pagliano Server and available server backups did not reveal any indications of malware.⁵²⁶

(U//~~FOUO~~) On January 9, 2011, Cooper sent Abedin an e-mail stating someone was attempting to “hack” the server, prompting him to shut it down.⁵²⁷ Cooper sent Abedin another e-mail later the same day stating he had to reboot the server again.⁵²⁸ The FBI's investigation did not identify successful malicious login activity associated with this incident.⁵²⁹

(U//~~FOUO~~) The FBI's review of available Internet Information Services (IIS) web logs showed scanning attempts from external IP addresses over the course of Pagliano's administration of the server, though only one appears to have resulted in a successful compromise of an e-mail account on the server.⁵³⁰ Forensic analysis noted that on January 5, 2013, three IP addresses matching known Tor^{fff} exit nodes were observed accessing a user e-mail account on the Pagliano Server believed to belong to President Clinton staffer [redacted] FBI investigation indicated the Tor user logged in to [redacted] e-mail account and browsed e-mail folders and attachments.^{531,532} When asked during her interview, [redacted] stated to the FBI she is not familiar with nor has she ever used Tor software.⁵³³ FBI investigation to date was unable to identify the actor(s) responsible for this login or how [redacted] login credentials were compromised.⁵³⁴

b6
b7C

(U//~~FOUO~~) Forensic analysis of alert e-mail records automatically generated by CloudJacket revealed multiple instances of potential malicious actors attempting to exploit vulnerabilities on the PRN Server. FBI determined none of the activity, however, was successful against the server.⁵³⁵

(U//~~FOUO~~) Following the March 3, 2015 *New York Times* article publicly revealing Clinton's use of personal e-mail to conduct government business,⁵³⁶ the FBI identified an increased number of login attempts to the PRN Server and its associated domain controller.^{gggg,537} Forensic analysis revealed none of the login attempts were successful. FBI investigation also identified an

^{eeee} (U) Older versions of RDP had a vulnerability in the method used to encrypt RDP sessions. While security patches, if applied, have remedied these vulnerabilities, exposing RDP to direct connections could allow remote attackers the opportunity to guess login credentials.

^{fff} (U) Tor is free software allowing end users to direct their Internet traffic through a group of volunteer-operated servers around the world in order to conceal their location and Internet usage.

^{gggg} (U) A domain controller is a Microsoft server that responds to security authentication requests (logins, checking permissions, etc.) within a Windows domain.

increase in unauthorized login attempts into the Apple iCloud^{hhhh} account likely associated with Clinton's e-mail addressⁱⁱⁱ during this time period. Investigation determined all potentially suspicious Apple iCloud login attempts were unsuccessful.⁵³⁸ Additionally, PRN made various network changes to the PRN Server around March 7, 2015, to include disabling the server's public-facing VPN page and switching from SSL protocol to TLS to increase security.⁵³⁹ Staff also discussed the possibility of conducting penetration testingⁱⁱⁱⁱ against the PRN Server to highlight vulnerabilities in the network.⁵⁴⁰ The FBI interviewed an employee of the company with which PRN had discussed the issue. The employee stated that the topic was broached but that penetration testing against the PRN Server, ultimately, did not happen.⁵⁴¹

B. (U//~~FOUO~~) Cyber Analysis of Clinton's Mobile Devices

(U//~~FOUO~~) The FBI does not have in its possession any of Clinton's 13 mobile devices which potentially were used to send e-mails using Clinton's clintonemail.com e-mail addresses. As a result, the FBI could not make a determination as to whether any of the devices were subject to compromise. Similarly, the FBI does not have in its possession two of the five iPad devices which potentially were used by Clinton to send and receive e-mails during her tenure.^{542, 543, 544, 545} The FBI forensically examined two of the three iPads^{kkkk} it obtained and found no evidence of cyber intrusion.⁵⁴⁶

C. (U//~~FOUO~~) Cyber Targeting of Clinton's Personal E-mail and Associated Accounts

(S//~~OC/NF~~) Investigation identified multiple occurrences of phishing and/or spear-phishing e-mails sent to Clinton's account during her tenure as Secretary of State.⁵⁴⁷ [redacted]

b1
b3
b6
b7C

(S//~~OC/NF~~) Clinton received another phishing e-mail, purportedly sent from the personal e-mail account of a State official, [redacted]. The e-mail contained a potentially malicious link.⁵⁵² Clinton replied to the e-mail [redacted] stating, "Is this really from you? I was worried about opening it!"⁵⁵³ [redacted]
In a separate incident [redacted] Abedin sent an e-mail to [redacted] indicating Clinton was

b1
b3
b6
b7C

^{hhhh} (U//~~FOUO~~) Apple iCloud is a cloud storage medium available to users of Apple products. Clinton is known to have used Apple iPads during the course of her tenure, and hdr22@clintonemail.com was likely used as her AppleID to set up a new Apple device.

ⁱⁱⁱ (U//~~FOUO~~) While the NYT article did not reveal Clinton's e-mail address—and by default the domain name—it is very likely those who tried to gain access to the related Apple iCloud account searched for and found the e-mail address in open sources. News articles from 2013 contained a screenshot of Blumenthal's communication with "hdr22," thereby divulging Clinton's e-mail alias. Other outlets mentioned the domain name in articles but withheld Clinton's e-mail alias. Clinton's full e-mail address could therefore have been ascertained through piecing together various sources.

ⁱⁱⁱⁱ (U) Penetration testing, more commonly known as pentesting, is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit.

^{kkkk} (U//~~FOUO~~) The third iPad the FBI obtained was not actually used by Clinton. Shortly after it was purchased, it was given as a gift to a member of her staff, and therefore the FBI did not forensically examine the device.

^{lll} (U) RAT is a piece of software that facilitates remote operation of a computer system.

worried “someone [was] hacking into her email” given that she received an e-mail from a known [redacted] associate containing a link to a website with pornographic material.⁵⁵⁴ There is no additional information as to why Clinton was concerned about someone hacking into her e-mail account, or if the specific link referenced by Abedin was used as a vector to infect Clinton's device [redacted]

b6
b7C

(S)

[redacted] Open source information indicated, if opened, the targeted user's device may have been infected, and information would have been sent to at least three computers overseas, including one in Russia.^{560,56} [redacted]
[redacted]

b1
b3

D. (U//~~FOUO~~) *Potential Loss of Classified Information*

(U//~~FOUO~~) On March 11, 2011, Boswell sent a memo directly to Clinton outlining an increase since January 2011 of cyber actors targeting State employees' personal e-mail accounts.⁵⁶³ The memo included an attachment which urged State employees to limit the use of personal e-mail for official business since “some compromised home systems have been reconfigured by these actors to automatically forward copies of all composed e-mails to an undisclosed recipient.”⁵⁶⁴ Clinton's immediate staff was also briefed on cybersecurity threats in April and May 2011.⁵⁶⁵

(S//~~OC/NF~~) [redacted]

b1
b3
b6
b7C
b7E

(S//~~OC/NF~~) [redacted]

b1
b3
b6
b7C
b7E

^{mmmm} (U) In order for malicious executables to be effective, the targeted host device has to have the correct program/applications installed. If, for example, the host is running an older version of Adobe but the exploit being used is newer, there is a chance the host will not be infected because the exploit was unable to execute using the older version of the program.

ⁿⁿⁿⁿ (U) A “drop” account, in this case, is an e-mail account controlled by foreign cyber actors and which serves as the recipient of auto-forwarded e-mails from victim accounts.

(U//~~FOUO~~) On or about March 14, 2013, Blumenthal's AOL e-mail account was compromised by Marcel Lehel Lazar, aka Guccifer, a Romanian cyber hacker. Lazar disseminated e-mails and attachments sent between Blumenthal and Clinton to 31 media outlets, including a Russian broadcasting company.⁵⁸⁷ [redacted]

b7E

[redacted]⁵⁸⁸ One of the screenshots captured a list of 19 foreign policy and intelligence memos authored by Blumenthal for Clinton.⁵⁸⁹ The content of one of the memos on the list was determined by State to be classified at the CONFIDENTIAL level.⁵⁹⁰ Lazar was extradited from Romania to the United States on March 31, 2016.⁵⁹¹

(U//~~FOUO~~) Between April 25, 2016 and May 2, 2016, Lazar made a claim to FOX News that he used information from Blumenthal's compromise as a stepping stone to hack Clinton's personal server.⁵⁹² On May 26, 2016, the FBI interviewed Lazar, who admitted he lied to FOX News about hacking the Clinton server.⁵⁹³ FBI forensic analysis of the Clinton server during the timeframe Lazar claimed to have compromised the server did not identify evidence that Lazar hacked the server.⁵⁹⁴ An examination of log files from March 2013 indicated that IP addresses from Russia and Ukraine attempted to scan the server on March 15, 2013, the day after the Blumenthal compromise, and on March 19 and March 21, 2013.⁵⁹⁵ However, none of these attempts were successful, and it could not be determined whether this activity was attributable to Lazar.⁵⁹⁶

E. (U//~~FOUO~~) General Cyber Analysis Conducted

(S//~~OC/NF~~) [redacted] The FBI conducted general cyber research and analysis of e-mail addresses and user accounts associated with the clintonemail.com and presidentclinton.com domains.

b1
b3
b6
b7C
b7E

(U//~~FOUO~~) FBI extracted the Thread-Index⁰⁰⁰⁰ and Message-ID^{pppp} values for each identified confirmed classified e-mail relevant to this investigation. The values were extracted from the e-mail headers^{qqqq} in order to develop specific electronic signatures that could be used when searching for exact references in large data repositories. In an effort to identify whether any confirmed classified e-mails may have been compromised through computer intrusion methods, the FBI conducted signature-based searches in available databases, to include [redacted]^{rr}. The FBI also provided the unique identifiers to other government agencies, and one entity

b7E

⁰⁰⁰⁰ (U) A Thread-Index value is a unique, alphanumeric, Microsoft Outlook-centric field found in an e-mail's header. The identifier is used to track e-mail threads (or conversations). Each time there is a reply or forward in the e-mail thread, Outlook—if it is the e-mail client being used—will append additional alphanumeric characters to the e-mail's original Thread-Index value.

^{pppp} (U) A Message-ID is a unique identifier found in an e-mail's header. Message-IDs are required to have a specific format and be globally unique. Unlike Thread-Index values, Message-IDs are unique to every individual e-mail, regardless of whether two e-mails belong to the same thread (or conversation).

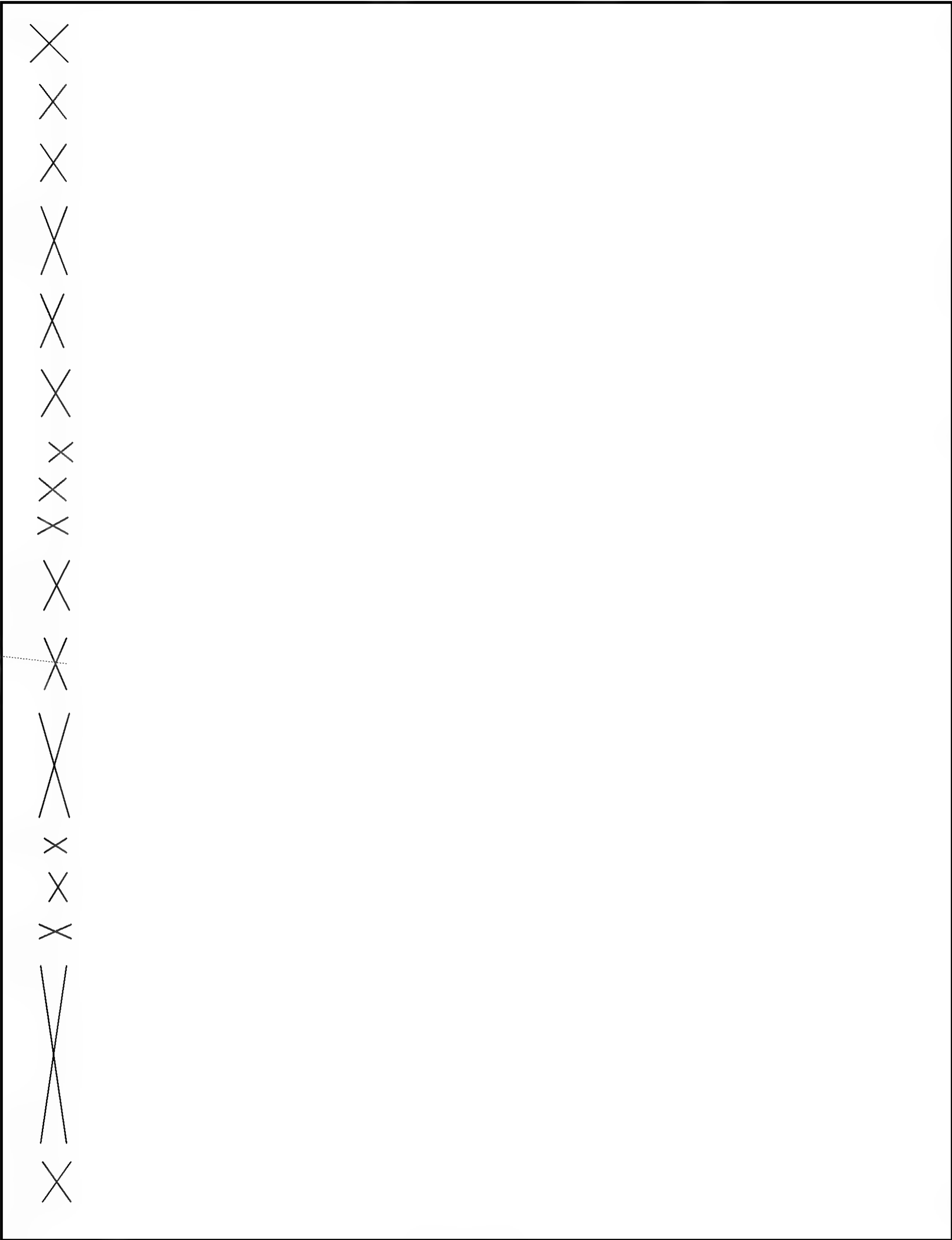
^{qqqq} (U) A header precedes the body (content text) of an e-mail, and contains lines (metadata) that identify particular routing information. Fields such as "From," "To," and "Date" are mandatory, while others are optional.

^{rr} (U//~~FOUO~~) [redacted]

b7E

responded.^{ssss} To date, the signature-based searches in USG databases have not identified the relevant e-mails.⁶⁰¹

^{ssss} (U//~~FOUO~~) The FBI provided the Executive Office of the President (EOP), State Cyber Threat Analysis Division (CTAD), and State's Information Resource Bureau (IRB) with Thread-Index and Message-ID values. CTAD found no record of the signatures provided. EOP stated they could only search "To," "From," and "Subject" lines, as did State IRB. Separately, in an attempt to identify whether confirmed classified e-mails resided in unidentified e-mail provider accounts, or whether identified accounts forwarded or replied to the classified messages, the FBI explored the possibility of sharing Thread-Index Value and Message-IDs with e-mail service providers of interest. Google was asked if they could search those header fields in its dataset. The company stated it does not index Thread-Index values, which is the identifier the FBI was most interested in, as it would have provided insight into the extent the messages were forwarded.



b3
b5
b6
b7C
b7E

Page 35 of 47

~~SECRET//ORCON/NOFORN~~

b1
b3
b5
b6
b7C
b7E

b1
b3
b7E

b1
b3
b5
b6
b7C
b7E

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON/NOFORN~~

X

X

X

X

X

x

x

x

X

X

x

X

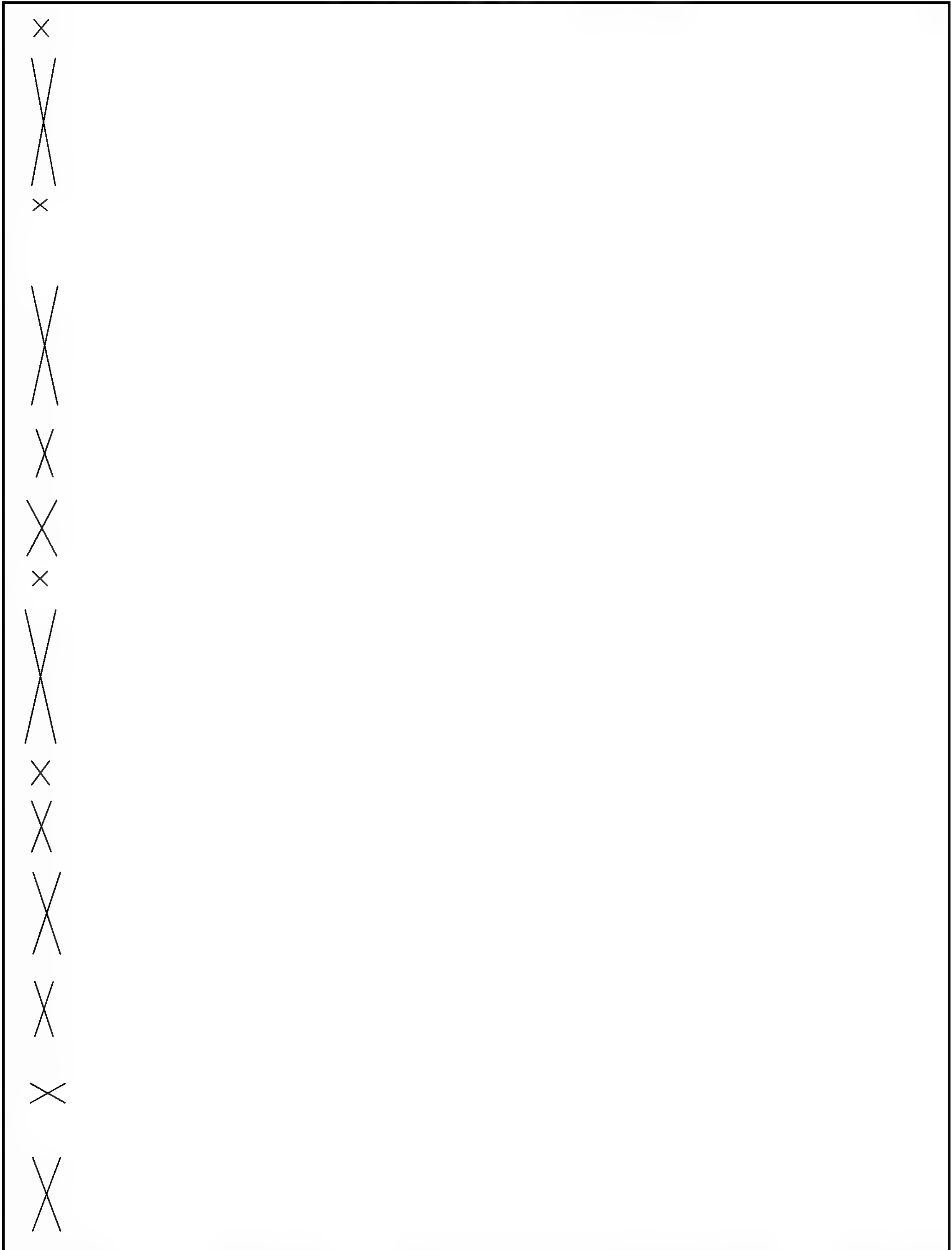
x

x

x

X

X





b1
b3
b7E

(U)

X

X

X

X

X

X

b3
b5
b6
b7C
b7E



b1
b3
b7E



b1
b3
b7E

(U)

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

X

b3
b5
b6
b7C
b7E



b1
b3
b7E

X

X

X

X

(U)

X

X

x

x

X

x

X

X

X

X

x

X

X

x

X

X

X

b3
b5
b6
b7C
b7E

b1
b3
b7E

(U)

X
X
X
x
X
x
X
x
X
x
X
x
X
X
X
x
x
X
x
x
X
X
X
x
X
x
X
x
X
X

b3
b5
b6
b7C
b7E

b1
b3
b7E

b3
b5
b7E

b1
b3
b7E



b1
b3
b7E

(U)

X
X

X
X

X
X
X
X
X
X
X
X
X
X

X
X

X
X
X
X
X
X
X
X
X
X

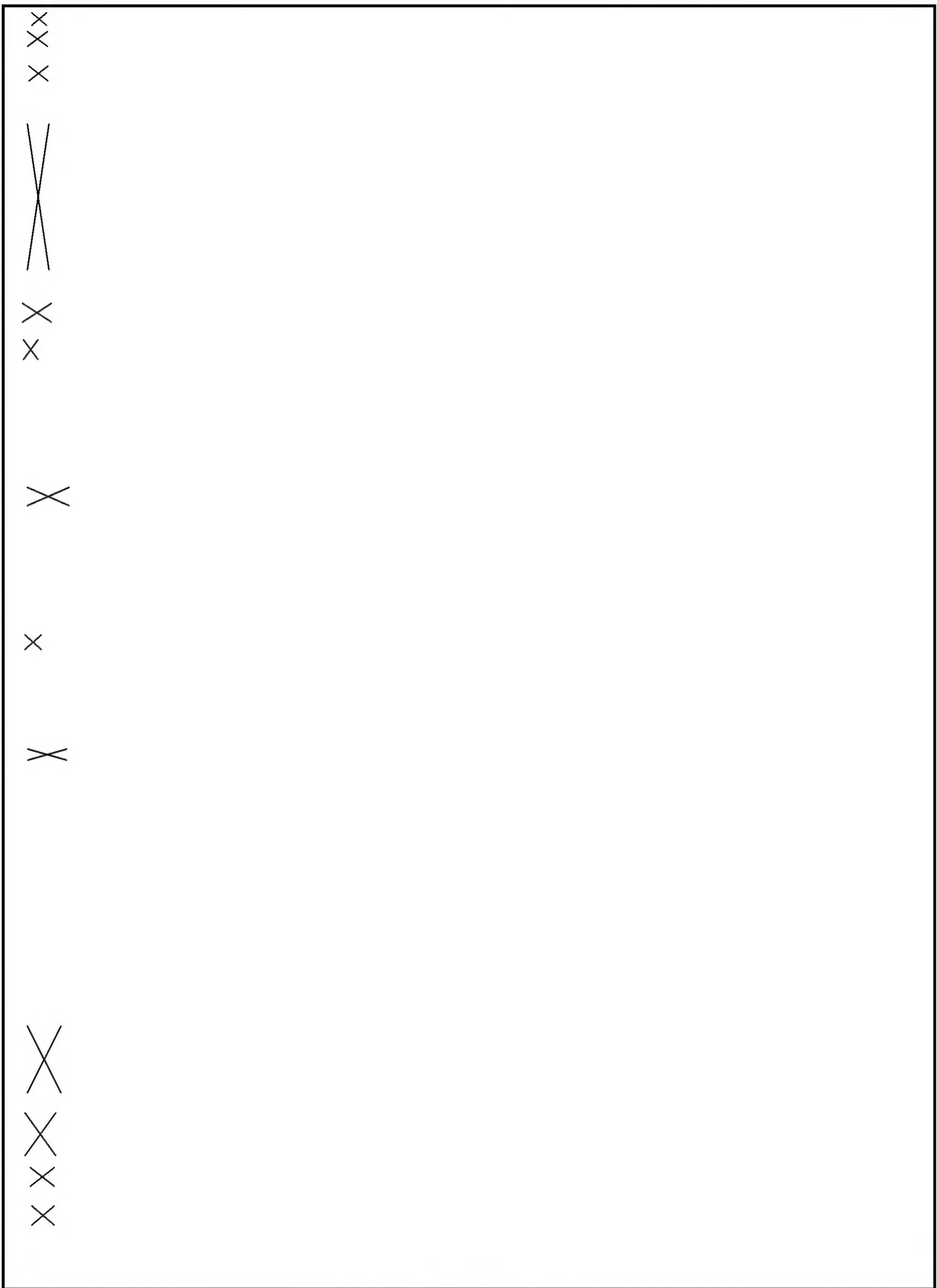
X

b3
b5
b6
b7C
b7E



b1
b3
b7E

b1
b3
b7E



b1
b3
b5
b6
b7C
b7E

b1
b3
b7E



X	
X	
X	
X	
X	
X	
X	
X	
X	

